

Département des Systèmes d'Information

Numéro de marché : 2025DGEDSSA058

MARCHE DE FOURNITURE ET SERVICE
Procédure avec négociation

Hébergement et TMA des applications Web et Mobile de
CertDc

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Inserm

Administration du Siège - Pôle Finances

101 rue de Tolbiac

75 654 Paris Cedex 13.

Table des matières

1.	Glossaire.....	4
2.	Préambule.....	6
2.1.	Objet du document.....	6
2.2.	Durée du marché.....	6
3.	Contexte du marché.....	8
3.1.	Présentation des parties prenantes du marché.....	8
3.1.1.	Présentation générale de l’Inserm.....	8
3.1.2.	Présentation générale de la direction générale de la santé (DGS) et du centre de crises sanitaires (CCS)	12
3.1.3.	Présentation générale de la Délégation au Numérique en Santé (DNS)	12
3.2.	Présentation des applications CertDc	13
3.2.1.	Éléments d’introduction aux certificats de décès	13
3.2.2.	Présentation de CertDc	14
4.	Présentation du marché	25
4.1.	Enjeux et objectifs	25
4.1.1.	Maintenabilité et évolutivité.....	26
4.1.2.	Respect des normes et standards	28
4.2.	Périmètre des prestations du marché.....	32
4.3.	Planning prévisionnel	32
5.	Description des prestations attendues	34
5.1.	Prestation 1 : Prise de connaissance et transfert de compétences	34
5.1.1.	Objectif.....	34
5.1.2.	Description	34
5.1.3.	Livrables	35
5.2.	Prestation 2 : Migration des environnements, applications et des données.....	35
5.2.1.	Objectif.....	35
5.2.2.	Description	36
5.2.3.	Livrables	38
5.3.	Prestation 3 : Hébergement et exploitation des applications web et mobile de CertDc.....	38
5.3.1.	Dispositions générales d’hébergement	39
5.3.2.	Performances	39
5.3.3.	Disponibilité et niveaux de service	39
5.3.4.	Sécurité et protection des données.....	40
5.3.5.	Audit.....	43
5.3.6.	Évolutivité et maintenance de l’infrastructure technique.....	43
5.3.7.	Support technique	44

5.4.	Prestation 4 : Tierce Maintenance Applicative Corrective et Préventive des applications mobile et Web de CertDc	45
5.4.1.	Objectif	45
5.4.2	Maintenance corrective	46
5.4.3	Maintenance préventive	49
5.4.4	Livrables	50
5.5	Prestation 5 : Tierce Maintenance Applicative Evolutive et Adaptative des applications web et mobile de CertDc	50
5.5.1	Objectif	50
5.5.2	Modalités de commande et d'exécution des prestations	51
5.5.3	Livrables	53
5.6	Prestation 6: Réversibilité sortante	53
5.6.1	Objectif	53
5.6.2	Description	53
5.6.3	Livrables	55
6	Suivi opérationnel des prestations	56
6.1	Description	56
6.2	Comitologie	56
6.3	Dispositif humain	57
6.4	Livrables	57
7	Modalités pratiques de la prestation	57
7.1	Horaires et disponibilité du titulaire	57
7.2	Langues	58
7.3	Changement du périmètre	58
8	Annexes	59

1. Glossaire

ARS	Agence Régionale de Santé
ANS	Agence du Numérique en Santé
ASIP	Accueil Social Inconditionnel de Proximité
CCS	Centre de crises sanitaires
CépiDc	Centre d'épidémiologie sur les causes médicales de décès
CertDc	Certification électronique des décès
DINUM	Direction Interministérielle du Numérique
DR	Délégation régionale
DSI	Département du Système d'Information
EPST	Etablissement Public à caractère Scientifique et Technologique
ES	Etablissement de santé
ESMS	Établissement ou service social ou médico-social
FAQ	Foire aux questions
FINESS	Fichier National des Etablissements Sanitaires et Sociaux
IDE	Infirmier.e Diplômé.e d'Etat
IML	Institut Médico-Légal
INSEE	Institut National de la Statistiques et des Etudes Economique
INSERM	Institut National de la Santé et de la Recherche Médicale
MSSANTE	Messagerie Sécurisée de Santé
OEC	Officier d'Etat Civil
OS	Operating system
HUBEE	Hub d'échange de l'état
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
POF	Portail Opérateur Funéraire
PGSSI-S	Politique Générale de sécurité des Systèmes d'information de Santé
PSSIE	Politique de sécurité des systèmes d'information de l'État
RGAA	Référentiel général d'accessibilité pour les administrations
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel général de sécurité
ROF	Référentiel Opérateur Funéraire
RPPS	Répertoire Partagés des Professionnels de Santé
SADL	Service d'appui aux délégations régionales et aux laboratoires
SAG	Service des affaires générales
SCSI	Service cohérence du SI
SNDS	Système National des Données de Santé
SSDUN	Service solutions et développement des usages numériques
SP FRANCE	Santé Publique France (ex-Institut National de Veille Sanitaire)
SPI	Service de la production infogérée
SSO	Single Sign-On (en français : authentification unique)
TMA	Tiers Maintenance Applicative
USAR	Unité surveillance et anticipation des risques

VA	Volet Administratif (certificat de décès)
VM	Volet Médical (certificat de décès)
VSR	Vérification de Service Régulier

2. Préambule

2.1. Objet du document

Le présent marché a pour objet l'assistance à maîtrise d'œuvre pour les prestations suivantes :

- Prestation 1 : Prise de connaissance et transfert de compétences.
- Prestation 2 : Migration des environnements.
- Prestation 3 : Hébergement et exploitation des applications web et mobile de CertDc.
- Prestation 4 : Tierce Maintenance Applicative Corrective et Préventive des applications mobiles et Web de CertDc.
- Prestation 5 : Tierce Maintenance Applicative Evolutive et Adaptative des applications mobiles et Web de CertDc.
- Prestation 6 : Réversibilité (transfert de connaissances).

Le marché se compose d'un unique lot et sera donc attribué à un seul titulaire, qui devra ainsi avoir la capacité d'assurer l'ensemble des prestations décrites ci-dessus. Il pourra sous-traiter certaines activités sous réserve de respecter les exigences décrites dans le CCAP sur ce sujet et après transmission des informations requises (voir formulaire DC4 dédié dans le DCE).

Les prestations 1, 2, 3, 4 et 6 sont forfaitaires tandis que la prestation 5 est à bons de commande.

2.2. Durée du marché

La durée du présent marché est de 2 ans fermes à compter de la date de notification, avec la possibilité de le renouveler tacitement deux fois pour une durée d'un an.

La tranche ferme comprend :

- La prestation 3 d'Hébergement et d'exploitation des applications web et mobile de CertDc, pour une durée de 2 ans.
- La prestation 4 de Maintenance de TMA Corrective et Préventive des applications de CertDc qui dure 2 ans.
- La prestation 5 de Maintenance de TMA Evolutive et Adaptative des applications de CertDc qui dure 2 ans.

La tranche optionnelle comprend :

- La prestation 1 de Prise de connaissance et de transfert de compétences (réversibilité entrante) et la prestation 2 de Migration des environnements sur l'hébergement du nouveau titulaire : **Ces deux prestations seront considérées comme fermes pour tout nouveau titulaire différent du précédent.**
- Le renouvellement de chacune des prestations 3, 4 et 5 pour une durée de 1 an avec la possibilité de renouveler 2 fois.
- La prestation 6 de Réversibilité sortante : cette prestation sera activée en fin de marché, en cas de non-renouvellement du titulaire.

La prestation devrait démarrer au plus tard 15 jours ouvrés après sa notification.

Le titulaire ne peut refuser une reconduction ou l'activation d'une prestation de la tranche optionnelle. Il ne peut pas s'opposer à la reconduction ou à la non-reconduction du marché. La décision de reconduction ou non-reconduction n'ouvre droit à aucune indemnité au profit du titulaire.

La personne responsable du marché se prononce au plus tard un mois avant la fin de la durée de validité du marché et notifie, par email avec accusé de réception ou par lettre avec accusé de réception, sa décision de ne pas reconduire le marché au titulaire.

3. Contexte du marché

L'application CertDc a été créée en 2006 à la suite de la canicule de 2003. Son objectif original était d'accélérer la remontée des causes médicales de décès inscrites dans les certificats de décès en proposant une interface informatisée (Web et MOBILE) de saisie des certificats de décès avec une transmission en temps réel. En 2022, l'application Web a entièrement été refondue. Aujourd'hui CertDc propose une gamme complète de fonctions :

- permettant aux professionnels de santé de rédiger des certificats de décès sur un système convivial, intuitif, conforme à l'état de l'art, offrant un design utilisateur enrichi et apte à supporter la charge tout en garantissant un haut niveau de sécurité.
- permettant aux référents d'établissement de santé (ES) et d'établissement médicaux-social (ESMS) d'effectuer les paramétrages adéquats en toute autonomie afin d'autoriser leur personnel à certifier des décès.
- offrant un niveau de performance capable d'absorber, sans dégradation des temps de réponse, l'augmentation du taux de dématérialisation généré par le déploiement de la transmission électronique des volets administratifs et des actions de conduite du changement.
- présentant un niveau de conformité satisfaisant les exigences et standards en vigueur au sein de l'administration et aux données de santé (PGSSI-S, RGS, RGPD, RGAA).
- basée sur une technologie maintenable et évolutive, autant sur le back office que le front office, et interfaçable avec le SI CépiDc.

Le présent marché a désormais pour objectif d'identifier un titulaire capable d'assurer l'ensemble des prestations décrites dans ce CCTP et permettre d'assurer le bon fonctionnement et l'évolution des solutions web et mobiles CertDc.

3.1. Présentation des parties prenantes du marché

3.1.1. Présentation générale de l'Inserm

L'Inserm est un Etablissement Public à caractère Scientifique et Technique (EPST), placé sous la double tutelle du ministère de la Recherche et du ministère de la Santé.

Sa mission est d'améliorer la compréhension des maladies et de raccourcir les délais pour faire bénéficier les patients, le monde médical et les partenaires nationaux et internationaux, des résultats de la recherche.

Ses domaines d'activité vont de la biologie fondamentale à la santé publique et son champ de compétence inclut toutes les dimensions fondamentales, médicales, cognitives, cliniques ou appliquées ayant trait à la recherche dans ces domaines.

L'Inserm est implanté en France sur environ 85 sites dont plus d'une trentaine sous sa responsabilité pour ce qui concerne l'administration des réseaux et des services associés. En 2025, l'Inserm compte 349 structures de recherche (CIC, IFR, U, US) dont 278 unités de recherche. Parmi les 278 unités, il y a 1140 équipes de recherche labellisées essentiellement localisées dans les universités et les centres hospitalo-universitaires français. Ces 349 structures de recherche sont mixtes et 26 000 personnes y travaillent. Le personnel est composé de 6 100 salariés de l'Institut, de chercheurs d'autres EPST (CNRS, INRA...), d'universitaires, de chercheurs étrangers, d'étudiants et doctorants.

L'administration centrale dont le siège est situé 101 rue de Tolbiac à Paris, est composée d'une dizaine de départements et services autour de la Direction Générale. Pour gérer ses structures de recherche, l'Inserm s'est doté de 13 Délégations Régionales (DR).

Tout complément d'information est disponible sur le site institutionnel : <https://www.inserm.fr>

3.1.1.1 Présentation générale du CépiDc

Le CépiDc, Centre d'épidémiologie sur les causes médicales de décès, unité de service de l'Inserm, a pour mission de produire la base de données statistique sur les causes médicales de décès en France, de la diffuser et de réaliser des analyses sur cette base de données.

Cette base de données statistique repose sur la collecte et le traitement des volets médicaux des certificats de décès. Cette mission est encadrée par la loi nationale (Articles L2223-42 et R2213-1 du code des collectivités territoriales) qui assure le rôle de l'Inserm dans la collecte de l'information et précise les finalités d'usage des données. Ces finalités sont la veille et l'alerte sanitaire, l'établissement de la statistique nationale des causes de décès et la recherche en santé publique, l'alimentation du système national des données de santé, l'établissement de statistiques dans le cadre de l'article 7bis de la loi de 1951. Ainsi, au niveau national, les données collectées et traitées par le CépiDc sont mobilisées à des fins de veille sanitaire, de statistiques publiques et de recherche.

Cette mission est aussi encadrée au niveau international. La statistique sur les causes de décès est soumise au règlement CE 1338/2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail et au règlement d'application 328/2011. Selon ces règlements, la collecte doit suivre les recommandations de l'Organisation mondiale de la Santé (OMS). La statistique doit être codée dans la classification internationale des maladies de l'OMS ; les normes d'évaluation de la qualité sont celles du code des bonnes pratiques en matière de statistique européenne ; les concepts, champs, variables, périodes de référence et délais de transmission sont fixés. De ce fait, le CépiDc est considéré comme une « autorité statistique nationale », productrice de statistique officielle, hors service

statistique public, auquel s'applique aussi le règlement UE 223, dont le code des bonnes pratiques en matière de statistique européenne découle.

Le CépiDc est membre du Centre Collaborateur français de l'OMS pour la Famille des Classifications Internationales (FIC) de laquelle la classification internationale des maladies découle et membre de l'Iris Core Group, groupe de pays en charge de maintenir et développer le logiciel international de codage automatique des causes médicales de décès IRIS.

Les informations relatives aux décès sont très utilisées en matière d'alerte sanitaire (Agences régionales de santé et Santé Publique France (ex-Institut National de Veille Sanitaire)), avant d'être exploitées en termes de veille et recherche épidémiologique.

Le CépiDc est maître d'ouvrage en ce qui concerne le volet médical du certificat de décès. En particulier, il est en charge d'assurer que le questionnaire de ce volet médical est conforme aux standards internationaux et que la collecte satisfasse les critères de qualité pour que l'information collectée soit la plus fiable et pertinente possible.

3.1.1.2 Présentation du Département du Système d'Information (DSI)

Le département système d'information (DSI) définit, met en œuvre et coordonne la politique en matière de système d'information.

Ses missions sont les suivantes :

- Elaborer l'architecture du système d'information destiné au pilotage et à la gestion des différentes activités de recherche et d'appui de l'établissement.
- Définir les moyens techniques et organisationnels permettant de mettre en œuvre la politique en matière de système d'information.
- Conseiller et accompagner les unités sur la mise en œuvre des technologies de l'information.
- Assister les maîtrises d'ouvrages pour traduire l'expression de leurs besoins fonctionnels en projets de développement applicatif et de conduire ces projets.
- Proposer, en concertation avec les directions opérationnelles et fonctionnelles, la politique en matière d'achat de biens et services dans le domaine des technologies de l'information.
- Piloter et coordonner la politique sécurité des systèmes d'information en s'assurant de l'efficacité et de la maîtrise des risques, et de manière générale du maintien en conditions opérationnelles du système d'information.

Pour assurer ses missions, le DSI est chargé de l'élaboration du schéma directeur du système d'information et, après approbation par le comité directeur du système d'information, du suivi de sa mise en œuvre.

Le DSI fournit une vision globale des actions et des dépenses liées aux systèmes d'information. Il tient à jour la cartographie du système d'information et anticipe les évolutions nécessaires. Il évalue et préconise les investissements à réaliser en fonction des évolutions technologiques.

Le champ de compétence du DSI s'étend à l'ensemble du système d'information de l'établissement et couvre le pilotage, la production, les projets et la prospective en matière de système d'information. Pour autant, le département collabore plus spécifiquement avec un certain nombre de directions métiers.

Le Département du Système d'Information (DSI) est un département de l'Inserm. Il définit, met en œuvre et coordonne la politique de l'Inserm en matière des systèmes d'information. Il est organisé en services et en missions couvrant tout son périmètre de compétence. On y trouve :

- Service cohérence du SI (SCSI).
- Service solutions et développement des usages numériques (SSDUN).
- Service de la production infogérée (SPI).
- Service d'appui aux délégations régionales et aux laboratoires (SADL).
- Service des affaires générales (SAG).

Le DSI est le maître d'œuvre de ce projet dont le pilotage est assuré par le service SSDUN et SPI.

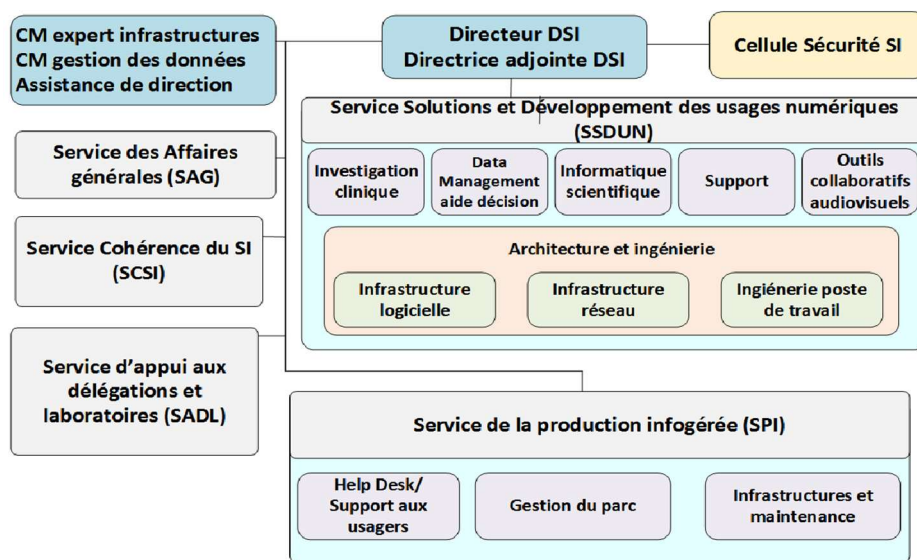


Figure 1 - Organisation de la DSI INSERM

3.1.2. Présentation générale de la Direction Générale de la Santé (DGS) et du centre de crises sanitaires (CCS)

La Direction Générale de la santé (DGS) prépare la politique de santé publique et contribue à sa mise en œuvre. Son action se poursuit à travers 4 grands objectifs : préserver et améliorer l'état de santé des citoyens, protéger la population des menaces sanitaires, garantir la qualité, la sécurité et l'égalité dans l'accès au système de santé, et mobiliser et coordonner les partenaires.

Elle s'est dotée depuis le 1er mars 2024 d'un centre de crises sanitaires (CCS) dont les objectifs sont de consolider les capacités ministérielles en termes d'anticipation, de préparation et de gestion des alertes et des crises, tout en restructurant l'organisation ministérielle de crise. Il s'appuie sur l'expertise et les capacités d'action des autres entités de la DGS et des directions d'administration centrale, ainsi que sur les compétences des agences sanitaires, des agences régionales de santé, des sociétés savantes, des professionnels de santé et plus globalement de tous les partenaires de la sécurité sanitaire.

Il dispose d'un pôle de préparation aux crises qui assure la préparation, en amont, des situations sanitaires exceptionnelles et d'une unité d'anticipation des risques qui intègre des systèmes de surveillance performants et une communication efficace avec l'ensemble des partenaires, pour les situations le nécessitant.

Cette unité surveillance et anticipation des risques (USAR) est la maîtrise d'ouvrage stratégique de l'application CertDc dans le cadre de l'amélioration du dispositif national d'alerte sanitaire, devant permettre de recueillir et diffuser rapidement les informations relatives au décès auprès des acteurs de veille sanitaire régionaux et nationaux. Elle définit par ailleurs le plan d'action pour la généralisation de l'outil à l'ensemble des établissements de santé en lien avec les ARS ainsi que du volet administratif auprès de l'ensemble des acteurs (mairies, opérateurs funéraires, officiers de police judiciaire).

3.1.3. Présentation générale de la Délégation au Numérique en Santé (DNS)

Créée en 2019 pour assurer le pilotage de l'agence du numérique en santé (ANS) et la mise en œuvre opérationnelle de la politique du numérique en santé, la Délégation au Numérique en Santé (DNS) voit son statut et ses responsabilités renforcées en 2023 par décret. La DNS devient une direction rattachée au Ministère de la Santé dont le rôle est de définir et mettre en œuvre la stratégie du numérique en santé, en lien avec les autres directions et services des ministères chargés des affaires sociales.

Elle définit la stratégie qui permet d'accélérer le développement du numérique en santé, en lien avec les autres directions ministérielles et les acteurs du secteur.

Elle pilote la mise en œuvre opérationnelle et les chantiers de transformations comme la Feuille de route du numérique en Santé, Le Ségur du Numérique ou encore la stratégie d'accélération « Santé Numérique ».

Elle est garante de la co-construction permanente avec les acteurs de terrain et de la bonne coordination entre les acteurs publics régionaux, nationaux et internationaux.

Via le sous-pôle « Santé Publique & Situations Sanitaires Exceptionnelles » (SPSSE), la DNS pilote les SI de santé publique et apporte une expertise d'assistance à maîtrise d'ouvrage pour accompagner le métier de la DGS sur plan de l'expression des besoins et sur la compréhension des spécifications SI.

3.2. Présentation des applications CertDc

3.2.1. Eléments d'introduction aux certificats de décès

Le certificat de décès fait l'objet d'un fort encadrement juridique. Son contenu et sa forme sont définis par un arrêté du ministère chargé de la santé qui distingue d'ailleurs deux modèles de certificats de décès : l'un réservé aux décès néonataux (avant 28 jours de vie), l'autre à tous les autres décès. Ces deux modèles ont une partie d'informations communes et une partie d'informations spécifiques à chacun.

Le certificat de décès comprend deux volets (voir le modèle de certificat de décès annexé à ce document) ;

- Un volet administratif comprenant des informations relatives à l'identité du défunt. Ce volet est destiné à l'établissement des registres d'État civils, aux opérations funéraires, au suivi démographique.
- Un volet médical comprenant des informations médicales, notamment les causes de décès, écrites en texte libre et des informations complémentaires, destiné à la surveillance épidémiologique des causes médicales de décès.

Création de certificat

Volet administratif Volet médical Récapitulatif / validation

Les champs suivis d'un ** rouge sont obligatoires pour l'enregistrement
Les champs suivis d'un * marron sont obligatoires pour la validation du certificat

Date et heure de décès

Date et heure (réelle ou estimée) de la mort

Date * Heure *

A défaut (impossibilité à établir), date et heure constatée du décès

Date * Heure *

Lieu de décès

Code postal / Commune de décès *

75001 - PARIS 01

Causes du décès

Partie 1 : Maladie(s) ou affection(s) morbide(s) ayant directement provoqué le décès

a) *

b) Due à ou consécutive à

c) Due à ou consécutive à

Volet administratif Volet médical

Figure 2 Exemple de certificat de décès avec les deux volets : administratif et médical

3.2.2. Présentation de CertDc

CertDc (Certification électronique des décès) permet aux professionnels de santé autorisés (médecins libéraux et hospitaliers, internes et Infirmier.ère.s diplômé.e.s d'Etat (IDE)), de saisir les certificats de décès et de les transmettre à l'ensemble des acteurs concernés de manière dématérialisée. En effet, la déclaration traditionnelle des décès via un document papier ne permet pas de disposer rapidement des informations issues des certificats de décès, du fait du long circuit de transmission avec de nombreux intermédiaires.

La dématérialisation via CertDc permet une transmission rapide des informations au CépiDc et à l'ensemble des partenaires. L'utilisation de CertDc est à privilégier pour la certification des décès, elle est même obligatoire depuis le 1er juin 2022 dans certains cas ([Décret no 2022-284 du 28 février 2022](#)).

L'application CertDc est accessible depuis le site web (<http://www.CertDc.inserm.fr>) ou via une application mobile de type PWA (<https://CertDc.inserm.fr/mobile/santeConnect>).

Pour déclarer un décès, le professionnel de santé doit d'abord s'identifier avec sa Carte e-CPS ou Carte Professionnelle de Santé (CPS) ou en saisissant son identifiant et son mot de passe (voir Figure 3 ci-contre).



Figure 3 Page de connexion de l'application mobile

Ensuite, il remplit le volet administratif (VA), contenant les informations administratives du défunt (nom, sexe, date de naissance, lieu de décès etc.) ; le volet médical (VM) précisant les causes médicales du décès, ainsi que d'autres éventuels documents (ex : demandes d'autopsie, prélèvements, demande de mise en bière etc.).

L'application mobile est utilisée par les professionnels de santé amenés à réaliser des certificats de décès en itinérance et sans ordinateur à portée de main. L'application est utilisable hors connexion afin de permettre son utilisation dans des zones blanches ou reculées.

Les personnels de santé peuvent également transmettre leurs certificats de décès via des systèmes d'information partenaires.

Après validation, le certificat de décès est envoyé de manière dématérialisée à l'ensemble des acteurs concernés.

- Le volet médical est transmis au CépiDc de l'Inserm (www.cepide.inserm.fr/) pour analyse des causes de décès.
- Le volet administratif est transmis à la mairie du lieu de décès du défunt et aux opérateurs funéraires.

Le schéma ci-dessous récapitule le chemin suivi par le certificat de décès.

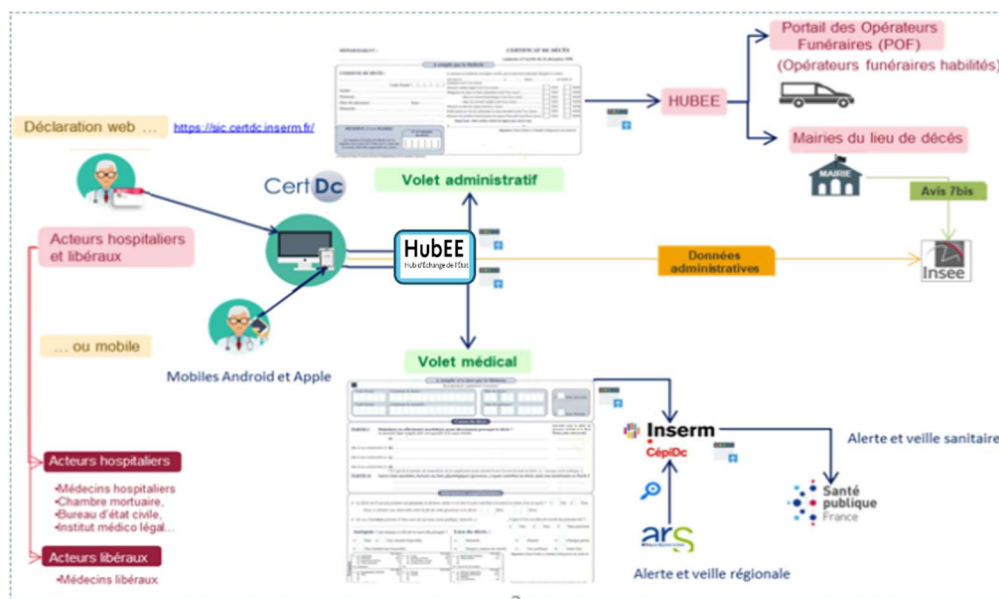


Figure 4 Chemin suivi par le certificat de décès

Le Site CertDc (http://www.CertDc.inserm.fr/accueil_public.php) dispose d'un mode test qui peut être utilisé pendant cette phase pour permettre au titulaire de découvrir l'application web et ses fonctionnalités.



Figure 5 Accueil du mode test de l'application

3.2.2.1 Chiffres clés et faits marquants

Le nombre de certificats de décès créés en France, chaque année, est d'environ 650 000.

Environ la moitié de ces certificats sont effectués par voie dématérialisée (applications web et mobile confondues).

En 2024, environ 32 000 professionnels de santé ont utilisé l'application (10 % médecins inscrits au Tableau de l'Ordre des Médecins).

Depuis 2024, les IDE répondant à certains critères d'éligibilité, peuvent également déclarer les décès via l'application CertDc. Cette population compte environ 500 000 professionnels et environ 40% de cette population utilisera l'application CertDC.

Le nombre maximal de sessions simultanées est estimé actuellement de 400 à 500 pour un nombre de visites moyen par jour constaté d'environ 50000 visites.

En 2025, plus de 5 500 mairies sont raccordées aux applications CertDc, ce qui leur permet de traiter les procédures d'état civil de manière dématérialisée. Les grandes métropoles (Paris, Lyon, Marseille, Bordeaux) sont toutes connectées au système CertDc.

La liste des mairies en cours de raccordement est disponible sur le site web de CertDc via le lien : <https://CertDc.inserm.fr/CertDc-public/#/mairies-etablissements-raccordes>

3.2.2.2 Acteurs de CertDc

Le tableau ci-dessous liste les acteurs de l'application CertDc et leur rôle. Cette liste n'est pas exhaustive, elle est donnée à titre indicatif et pourra être amenée à évoluer au cours du marché à venir.

Tableau 1 Cartographie des utilisateurs des applications

Organismes utilisateurs	Description et rôles
Médecins	Certification du décès
IDE (Infirmiers diplômés d'Etat)	Certification du décès
Référent	Paramétrer l'ES /ou l'ESMSM et les utilisateurs dans CertDc
Administrateur	Membre de l'Inserm. Il administre l'application CertDc
Mairies	Renseigner les registres d'Etat civil et établir un acte de décès
HUBEE	Plateforme d'échange de confiance opérée par la DINUM qui transmet les VA à la mairie du lieu de décès et au portail des opérations funéraires (POF)
CépiDC	Service de l'INSERM chargé de la production de la statistique sur les causes médicales de décès en France
POF	Plateforme de mise à disposition du VA aux opérateurs funéraires
INSEE	Organisme de statistique destinataire des traits d'identité des certificats de décès
IDNOW	Titulaire qui gère la génération des QRCode
ENOVACOM	Titulaire qui gère l'envoi des e-mails vers l'ASIP Santé

3.2.2.3 Cartographie logicielle synthétique de l'application web CertDc

Architecture fonctionnelle

L'application web CertDc est découpée en 5 quartiers fonctionnels :

- **Transverse** : Ce quartier regroupe les fonctionnalités transverses du système d'information CertDc.
- **Pilotage** : Ce quartier regroupe les fonctionnalités de statistiques et tableaux de bord.
- **Opérations** : Ce quartier correspond au cœur de métier de l'application, il regroupe les fonctionnalités liées à la gestion des certificats de décès.
- **Administration** : Ce quartier regroupe les fonctionnalités d'administration fonctionnelle de l'application.
- **Echange** : Ce quartier regroupe les fonctionnalités d'interfaçage avec les autres SI.

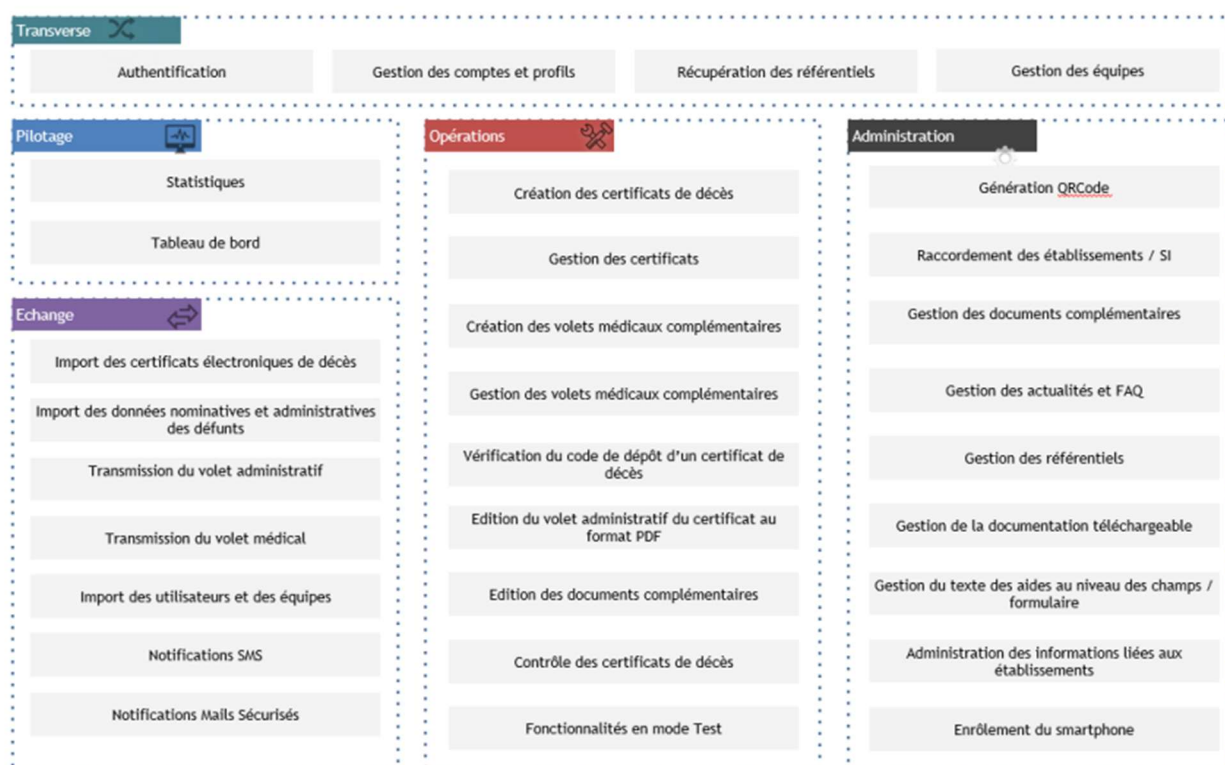


Figure 6 Cartographie du périmètre fonctionnel de l'application

Architecture logique

Le SI CertDc peut être découpé en plusieurs modules fonctionnels, regroupant les fonctionnalités ci-dessous :

- **Monitoring et mesure d'audience** (Statistiques et Tableau de bord).

- **Consultation** (Raccordement des SI, Rattachement des établissements, Actualités et FAQ).

- **Collecte et administration**

- Gestion des comptes et profils.
- Gestion des équipes.
- Import des certificats électroniques de décès depuis l'application « mobile ».
- Import des données nominatives et administratives des défunts (Passage de **contexte**).
- Création des certificats de décès.
- Gestion des certificats de décès.
- Gestion des référentiels.
- Gestion de la documentation téléchargeable.
- Gestion du texte des aides au niveau des champs / formulaire.
- Administration des informations liées aux établissements.
- Enrôlement du smartphone (pour utilisation de l'application « mobile »).

- **Batch et échanges de données**

- Récupération des référentiels.
- Transmission des données du volet administratif.
- Transmission des données du volet médical.
- Import des utilisateurs et des équipes.
- Notifications SMS.
- Notifications Mails sécurisés.
- Génération QRCode.
- Purge des Certificats.

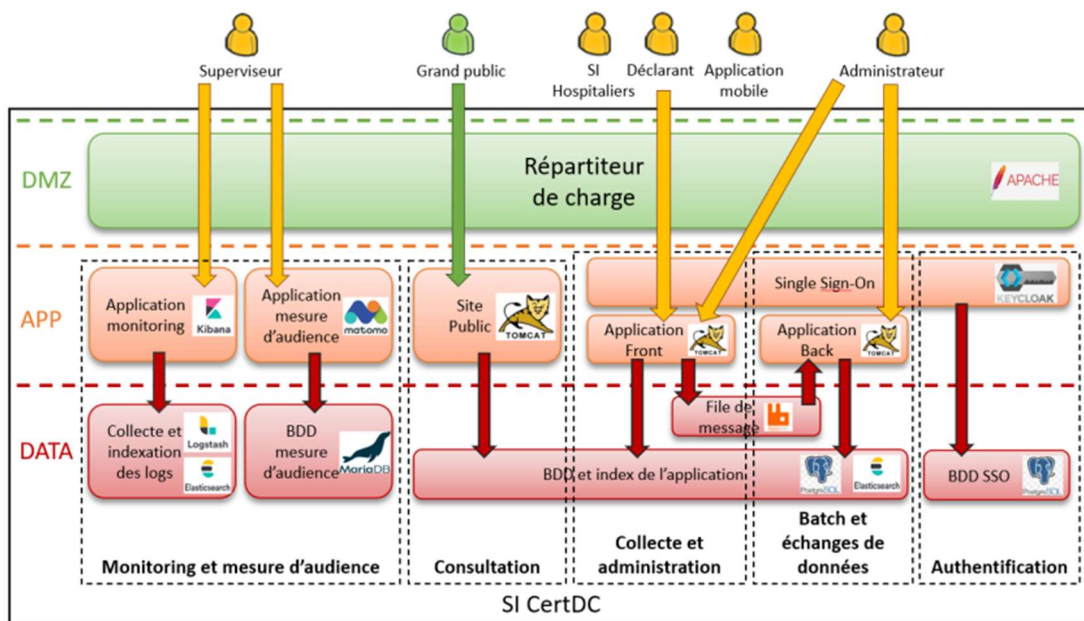


Figure 7: Schéma d'architecture logique

Flux externes de l'application web

En termes de flux de données, l'application CertDc propose :

- Une application front qui met à disposition des WS afin de s'interfacer avec :

- L'application mobile pour l'enrôlement du matériel utilisateur (smartphone, tablette voir PC portable) et l'import des certificats saisis.
- Les SI hospitaliers pour l'import des données nominatives de défunts (passage de contexte).
- Alinto pour l'envoi de SMS.
- AriadNext pour la génération de QrCode.
- Enovacom pour l'envoi de mails vers les messageries MSSANTE.

- Une application back qui concentre tous les batchs et permet de s'interfacer avec :

- RPPS pour la récupération des données de professionnels de Santé.
- AriadNext pour la génération de QrCode.
- Enovacom pour l'envoi de mails vers les messageries MSSANTE.
- Le CépiDc pour la transmission des données du volet médical.

- INSEE pour la transmission des données du volet Administratif.
- Le HubEE pour la transmission des télé dossiers à destination des mairies et du POF.
- Le FINESS pour la récupération du référentiel FINESS.
- Le Datanova de Laposte et le référentiel géographique du MESRI pour la récupération des communes.

- Un module SSO pour s'interfacer avec :

- Pro Santé Connect pour l'authentification avec carte CPS et e-CPS.
- Le SSO du portail Santé.

Le schéma ci-dessous représente les différentes applications qui composent le SI CertDc et les flux qu'elles gèrent. Le sens de la flèche correspond en sens de **circulation de l'information (flux entrant ou flux sortant)**.

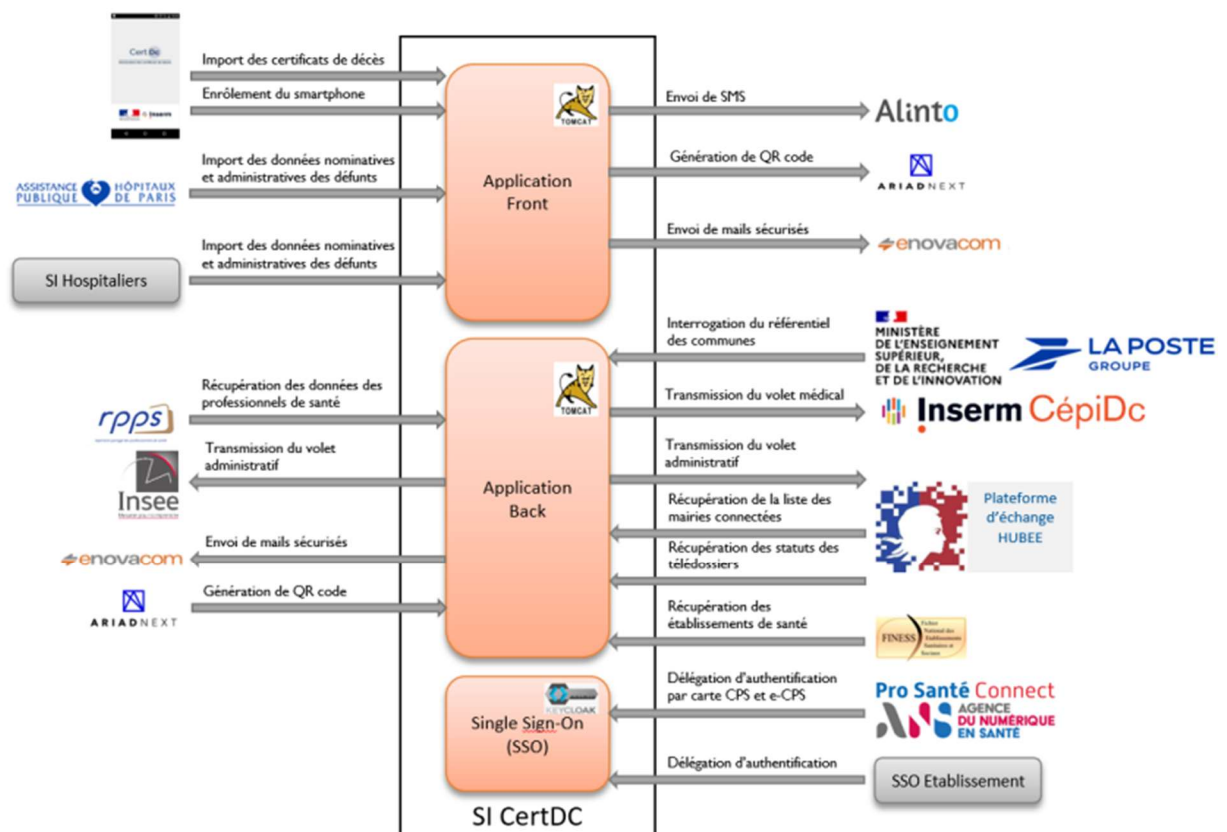


Figure 8 Cartographie des composants applicatifs et flux interapplicatifs

Architecture n-tiers

L'application web se base sur une architecture n-tiers, qui permet de la découper de façon logique en plusieurs couches. Chaque couche a un rôle déterminé et ne communique qu'avec les couches qui lui sont directement adjacentes.

Les couches sont présentées dans le schéma ci-dessous :

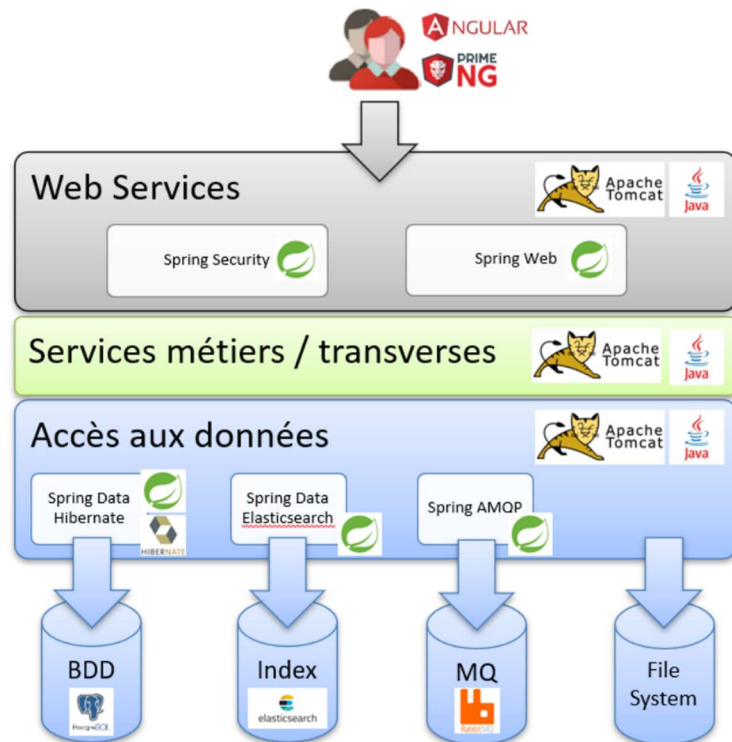


Figure 9 Couches d'architecture n-tiers

Postes clients

L'application web est actuellement accessible via un navigateur web dont les versions supportées sont les suivantes :

- Chrome 58+.
- Edge 14+.
- Firefox 54+.
- Safari 10+.
- Opera 55+.

Important

Le dossier d'Architecture Technique de l'application web CertDc sera communiqué au nouveau titulaire en début de marché.

3.2.2.4 Présentation synthétique de l'application mobile eCertDc

L'application mobile CertDc est de type PWA (Progressive Web App). Elle peut être installée sur l'écran d'accueil d'un smartphone sans avoir à passer par l'App Store ou Google Play.

Elle est capable de fonctionner selon un mode hors ligne, lorsque l'utilisateur est dans une zone non desservie et les actions réalisées seront synchronisées une fois l'appareil de nouveau connecté au réseau.

L'application eCertDc permet la saisie de certificats de décès. L'enregistrement de ces certificats se fait via l'envoi de ces derniers vers l'API du module frontal de l'application Web.

L'application mobile étant réécrite en une application PWA, elle est accessible à partir de n'importe quel périphérique (smartphone, tablette, ordinateur portable) disposant d'un navigateur internet, quel que soit son système d'exploitation (iOS, macOS, Android, Windows...).

Services tiers

L'application communique avec des Web services mis à disposition par CertDc Web. Ces communications entre l'application mobile et ces Web services seront utilisées pour les fonctionnalités suivantes :

- Enrôlement.
- Validation de certificats de décès.
- Récupération des mairies connectées.
- Récupération des établissements/profils d'un médecin.
- Récupération d'un token d'authentification.

Cette communication se fera en HTTPS. Le format d'échange des données est le JSON.

L'application utilise également l'API adresse.data.gouv.fr pour récupérer le code postal et la commune à partir de la géolocalisation de l'appareil.

Important

Le dossier d'Architecture Technique de l'application mobile eCertDc sera communiqué au nouveau titulaire en début de marché.

3.2.2.5 Ambition et projection sur les années à venir

Dans le cadre du développement de l'application CertDC, plusieurs axes d'évolution et d'ambition ont été définis. Ces orientations s'inscrivent dans une logique d'amélioration continue, tant sur le plan fonctionnel que sur le plan opérationnel.

- Evolution de l'outil
 - Affichage du résultat du codage automatique au cours de la saisie des causes de décès et préconisation pour en améliorer l'efficacité.
 - Accès au DMP du patient pour améliorer les causes de décès.
 - Transmission des causes de décès à toutes les ARS pour l'amélioration de la définition des politiques de santé publique.
 - Amélioration de la traçabilité des décès en ES (service, etc..).
 - Statistiques des nombres de décès déclarés par ES, services, équipes, médecin...
- Ambitions en matière de nombre d'ES et d'ESMS raccordés
 - Aujourd'hui environ 6 232 établissements (ES et ESMS) sont raccordés à CERTDC. Nous prévoyons une augmentation des raccordements de 30 % à 40% sur les 4 prochaines années.
- Ambitions en matière de taux de certification électronique
 - Au 1er trimestre 2025 le taux de certification électronique est de 51%. Nous visons d'atteindre :
 - 56% à fin 2025.
 - 82% à fin 2029 sur un rythme de croissance annuelle de 10%.
- Ambitions en matière de nbr de mairie raccordées :

-
- Au 1^{er} juillet 2025, il y a environ de 5500 mairies raccordées. Nous visons d'atteindre :
 - 5850 mairies raccordées fin 2025.
 - 8250 fin 2029 sur un rythme de croissance constant de 50 nouvelles mairies par mois.

4. Présentation du marché

4.1. Enjeux et objectifs

Ce marché vise à identifier le nouveau titulaire assurant les prestations d'hébergement, d'exploitation et de maintenance applicative (corrective, préventive, évolutive et adaptative, support) des deux applications CertDc mobile et Web dans les conditions et selon les exigences décrites dans la partie 5 de ce document.

Le marché vise à répondre aux enjeux suivants :

- Assurer la continuité de service de CertDc sans interruption significative, 7j/7, en particulier dans les établissements de santé et médico-sociaux.
- Garantir la sécurité et la traçabilité des données médicales et personnelles traitées par l'application.
- Apporter une capacité de maintenance corrective et évolutive réactive et fiable, en lien étroit avec la maîtrise d'ouvrage.
- Faciliter les évolutions réglementaires et fonctionnelles de l'application en conservant une qualité constante de service.
- Permettre à la MOA (DGS) de disposer de reportings clairs, d'indicateurs de performance, et d'un dialogue fluide avec le titulaire.

Sur l'hébergement, le titulaire du marché devra :

- Fournir un hébergement sécurisé, disponible, résilient, localisé en France.
- Garantir un taux de disponibilité mensuel minimal de 99,5 %, hors maintenances planifiées.
- Mettre en place une supervision technique 24/7, des mécanismes d'alerting et des sauvegardes conformes aux exigences du RGPD.
- Fournir un PRA/PCA documenté et testé au moins annuellement.
- Assurer la réversibilité complète des données et de l'environnement à l'échéance du marché.

Sur la TMA, le titulaire du marché devra :

- La maintenance corrective : prise en charge des incidents selon des SLA définis, résolution des anomalies bloquantes dans les délais impartis.
- La maintenance évolutive : analyse d'impact, chiffrage, mise en œuvre et livraison des évolutions fonctionnelles validées par la MOA.
- La maintenance préventive : supervision applicative, mises à jour techniques, traitement proactif des vulnérabilités, maintien de la cohérence technique des environnements.
- La gestion complète des environnements de recette, préproduction et production, en assurant leur synchronisation technique et fonctionnelle.

Sur la qualité de service et le suivi, le titulaire devra :

- Fournir des reportings périodiques incluant des indicateurs de performance (KPI) relatifs à la disponibilité, aux incidents, à la maintenance et aux évolutions.
- Participer aux comités de suivi TMA/hébergement organisés par la DGS et l'Inserm.
- Proposer, en tant que force de proposition, des revues d'architecture technique, des plans d'optimisation, et des recommandations proactives.

4.1.1. Maintenabilité et évolutivité

Ce chapitre vise à définir les exigences du pouvoir adjudicateur (DGS/INSERM) en matière de maintenabilité technique et d'évolutivité fonctionnelle et réglementaire de l'application CertDc dans le cadre du présent marché.

L'objectif est de garantir une application pérenne, adaptable, documentée et conforme aux bonnes pratiques, tant en termes de structure logicielle que de pilotage des évolutions.

Exigences en matière de maintenabilité

Le titulaire doit veiller à ce que l'application soit facile à maintenir, dans un souci de fiabilité, de maîtrise des coûts, de pérennité technologique et de sécurité.

Architecture technique maintenable

L'application doit reposer sur une architecture modulaire et documentée, permettant la localisation, l'isolement et la correction rapide des anomalies.

L'usage de design patterns standardisés, de frameworks maintenus (backend et frontend), et de bonnes pratiques de codage est requis.

Documentation technique à jour

Toute évolution (corrective ou évolutive) doit donner lieu à la mise à jour de la documentation technique associée:

- Schémas d'architecture.
- Spécifications fonctionnelles.
- Documentation des API.
- Journal des versions (changelog).

Tests automatisés et non-régression

Le titulaire doit maintenir une base de tests automatisés garantissant la stabilité du noyau applicatif (tests unitaires, fonctionnels, de non-régression).

Ces tests doivent être exécutés systématiquement avant toute mise en production.

Le taux de couverture des tests doit être suivi et documenté, notamment sur les fonctionnalités critiques (signature, certification, transmission des volets).

Suivi des évolutions et versioning

Chaque version de l'application (web et mobile) devra être horodatée et numérotée (version sémantique recommandée).

Un journal des évolutions (changelog) sera fourni pour chaque livraison, listant les correctifs, améliorations et nouvelles fonctionnalités.

Exigences en matière d'évolutivité

L'application CertDc est appelée à évoluer pour suivre :

- L'évolution du cadre réglementaire (lois santé, RGPD, décret décès, etc.).
- Les besoins fonctionnels nouveaux identifiés par la DGS et les utilisateurs.
- Les contraintes techniques (OS mobiles, navigateurs, socles systèmes).

Capacité d'intégration des évolutions

- L'architecture technique doit permettre un ajout de nouvelles fonctionnalités sans refonte lourde.
- Les APIs, services, et couches de données doivent pouvoir s'adapter aux nouveaux flux ou partenaires (SI hospitalier, Insee, opérateurs funéraires...).

Anticipation technologique

Le titulaire s'engage à :

- Réaliser une veille technologique sur les composants critiques (frameworks, OS, langages de développement, librairies).
- Proposer des plans de migration ou de montée de version en cas de risque d'obsolescence (ex : fin de support Android/iOS, fin de vie NodeJS, etc.).
- Réaliser au moins une revue technique annuelle sur la maintenabilité et l'évolutivité de l'application.

4.1.2. Respect des normes et standards

Les applications CertDc évoluent dans un contexte réglementaire où plusieurs normes sont applicables et doivent être respectées. Ainsi le titulaire doit maintenir et assurer la conformité des applications à ces normes et réglementations en vigueur et listées ci-dessous.

4.1.2.1 Politique de sécurité des systèmes d'information de l'État (PSSIE) et Politique Générale de sécurité des Systèmes d'information de Santé (PGSSI-S)

La **Politique de sécurité des systèmes d'information de l'État (PSSIE)** définit les exigences de sécurité applicables aux systèmes d'information utilisés par les administrations publiques. Elle est élaborée sous

l'égide de l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information) et vise à garantir la **confidentialité, l'intégrité, la disponibilité et la traçabilité** des données traitées par l'État.

La **PGSSI-S** (Politique Générale de Sécurité des Systèmes d'Information de Santé) est un cadre de référence mis en place par l'**Agence du Numérique en Santé (ANS)** pour sécuriser les systèmes d'information dans le domaine de la santé en France.

La documentation est disponible au lien ci-après: <https://esante.gouv.fr/securite/pgssi-s/espace-de-publication>.

4.1.2.2 Respect du Règlement Général sur la Protection des Données (RGPD)

Le RGPD est un règlement commun pour l'ensemble des pays de l'Union Européenne qui renforce les règles concernant la protection des données à caractère personnel.

L'objectif du RGPD est :

- d'une part, de renforcer les droits des personnes utilisant les outils en ligne contenant certaines de leurs informations personnelles. Une donnée personnelle est décrite par la CNIL comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il existe 2 types d'identifications :

- Identification directe (nom, prénom etc.),
- Identification indirecte (identifiant, numéro etc.).

- D'autre part, l'objectif du RGPD est de responsabiliser les acteurs traitant les données pour concevoir des outils respectant les règles définies.

Le titulaire, dans le cadre du marché, assure la conformité du SI au RGPD sur les points suivants :

- La transparence : A chaque donnée collectée, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information. Ces informations doivent permettre à l'utilisateur de comprendre pourquoi cette donnée est collectée, qui aura connaissance de cette donnée, le temps de conservation de la donnée ainsi que les modalités de traitement.
- Le consentement : Pour toute utilisation de données personnelles, le responsable du traitement doit être en mesure de prouver que l'utilisateur concerné a donné son consentement au traitement de ses données.
- La sécurisation des données : Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident. Les moyens pour garantir l'ensemble de la confidentialité et de l'intégrité des données doivent être mis en œuvre dès la phase conception de l'application.

De manière nominale, le RGPD impose aux applications de respecter des règles complètes en fonction des données et des traitements effectués.

La documentation sur cette norme est disponible au lien ci-après : [Le règlement général sur la protection des données - RGPD | CNIL](#).

4.1.2.3 Référentiel Général de Sécurité (RGS)

Le Référentiel Général de Sécurité (RGS) a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative.

Les applications CertDc sont homologuées RGS et **le titulaire assurera leur maintien en conformité**.

Le référentiel général de sécurité (RGS) vise à renforcer la confiance des usagers dans les services électroniques proposés par les autorités administratives, notamment lorsque ceux-ci traitent des données personnelles.

Il s'applique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et avec les usagers. Il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes.

Indirectement, le RGS s'adresse à l'ensemble des titulaires de services qui assistent les autorités administratives dans la sécurisation des échanges électroniques qu'elles mettent en œuvre. De façon générale, pour tout autre organisme souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques, le RGS se présente comme un guide de bonnes pratiques conformes à l'état de l'art.

Le RGS propose :

- D'une part une méthodologie orientée autour de la responsabilisation des autorités vis-à-vis de leurs systèmes d'information à travers la démarche d'homologation.
- D'autre part des règles et bonnes pratiques que doivent mettre en œuvre les administrations lorsqu'elles recourent à des prestations spécifiques : certification et horodatage électroniques, audit de sécurité.

Il comprend les règles permettant aux autorités administratives de garantir aux citoyens et aux autres administrations un niveau de sécurité de leurs systèmes d'information adapté aux enjeux et risques liés à la cybersécurité.

Il intègre les principes et règles liées à :

-
- La description des étapes de la mise en conformité.
 - La cryptologie et la protection des échanges électroniques.
 - La gestion des accusés d'enregistrement et des accusés de réception.
 - La qualification des produits de sécurité et des titulaires de services de confiance.
 - La validation des certificats par l'État.

La documentation relative à cette norme est disponible au lien ci-après [Le référentiel général de sécurité version 2.0 : les documents | ANSSI](#).

4.1.2.4 Référentiel général d'accessibilité pour les administrations (RGAA version 4.1*)

Il est important de prendre l'ensemble des contraintes d'accessibilité. Les applications doivent satisfaire à un niveau d'accessibilité exigé aujourd'hui par le RGAA (fonctionnel back et front-office, ergonomie, graphisme).

Le titulaire s'engage à mettre en œuvre et vérifier la conformité AA et à effectuer l'ensemble des tests associés aux points de contrôle définis dans le RGAA V4.1* et dans ses annexes en mettant en pratique les éléments liés à son guide d'accompagnement.

Un audit récent de l'application WEB atteste qu'à ce jour, 79% des critères d'accessibilité sont respectés et le titulaire s'engage à maintenir à minima ce seuil dans le cadre de ses développements.

L'accessibilité numérique consiste à rendre les services de communication au public en ligne accessibles aux personnes handicapées, c'est-à-dire :

- Perceptibles : par exemple, faciliter la perception visuelle et auditive du contenu par l'utilisateur ; proposer des équivalents textuels à tout contenu non textuel ; créer un contenu qui puisse être présenté de différentes manières sans perte d'information ni de structure (par exemple avec une mise en page simplifiée).
- Utilisables : par exemple, fournir à l'utilisateur des éléments d'orientation pour naviguer, trouver le contenu ; rendre toutes les fonctionnalités accessibles au clavier ; laisser à l'utilisateur suffisamment de temps pour lire et utiliser le contenu ; ne pas concevoir de contenu susceptible de provoquer des crises d'épilepsie.
- Compréhensibles : par exemple, faire en sorte que les pages fonctionnent de manière prévisible ; aider l'utilisateur à corriger les erreurs de saisie.
- Robustes : par exemple, optimiser la compatibilité avec les utilisations actuelles et futures, y compris avec les technologies d'assistance.

* La version 4.1 est la dernière en vigueur au moment de la rédaction du marché. Le titulaire s'engage à suivre toute évolution de la réglementation RGAA, à maintenir la compétence de ses équipes, et à soumettre au pouvoir adjudicateur toute proposition d'évolution visant à se conformer aux nouvelles normes.

4.2. Périmètre des prestations du marché

Les prestations prévues dans le marché sont les suivantes et sont décrites dans la partie [Description des prestations attendues](#) du présent document :

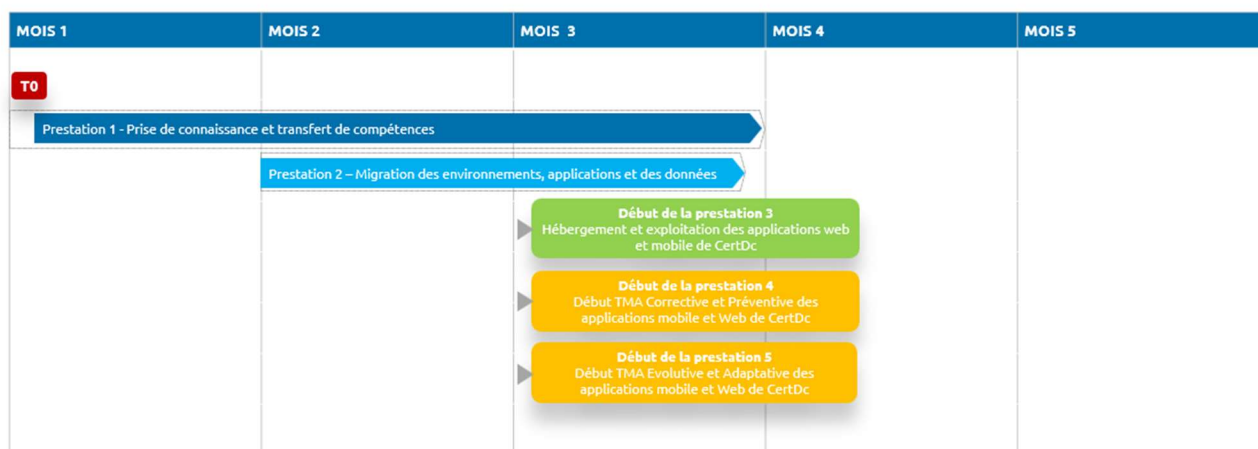
- Prestation 1 : Prise de connaissance et transfert de compétences.
- Prestation 2 : Migration des environnements.
- Prestation 3 : Hébergement et exploitation de l'application web et mobile de CertDc.
- Prestation 4 : Tierce Maintenance Applicative Corrective et Préventive des applications mobile et Web de CertDc.
- Prestation 5 : Tierce Maintenance Applicative Evolutive et Adaptative des applications mobile et Web de CertDc.
- Prestation 6 : Réversibilité sortante.

4.3. Planning prévisionnel

Le planning prévisionnel souhaité est le suivant :

- **Démarrage du projet : T0**
 - Comme évoqué précédemment, le T0 aura lieu au plus tard 15 jours après la notification du marché.
- **Prise de connaissance et transfert de compétences : T0 à (T0 + 3 mois)**
 - Prise de connaissance : T0 à (T0 +1 mois).
 - Transfert de compétences : (T0 +1 mois) à (T0+3 mois).
- **Migration des environnements, des données et des applications : de (T0 + 1 mois) à (T0 + 3 mois)**
 - Préparation de l'hébergement : (T0 + 1 mois) à (T0 + 2 mois).
 - Migration des données et des applications : (T0 + 2 mois) à (T0 + 3 mois).

- **Hébergement et exploitation des applications web et mobile de CertDc: de (T0 + 3 mois) à (T0+2 ans)** renouvelable tacitement 2 fois pour une durée d'un an (au plus tard (T0 + 4 ans)).
- **TMA Corrective et Préventive des applications mobiles et web de CertDc : (T0 + 3 mois) à (T0 + 2 ans)** renouvelable tacitement 2 fois pour une durée d'un an (au plus tard T0 + 4 ans).
 - Début TMA Corrective et Préventive à (T0 +2 mois), dont 1 mois sous la supervision de l'ancien titulaire, suivi d'1 mois -de (T0 +2 mois) à (T0 + 3 mois)-, en parallèle de la phase de transfert de compétences.
- **TMA Evolutive et Adaptative des applications mobiles et web de CertDc : (T0 + 3 mois) à (T0 + 2 ans)** renouvelable tacitement 2 fois pour une durée d'un an (au plus tard T0 + 4 ans).



- Début TMA Evolutive et Adaptative (T0 +2 mois), dont 1 mois sous la supervision de l'ancien titulaire, suivi d'1 mois -de (T0 +2 mois) à (T0 + 3 mois)- en parallèle de la phase de transfert de compétences.

Vous trouverez ci-dessous, à titre indicatif, le planning et les délais de réalisation des différentes phases du projet, objets du présent marché :

Le soumissionnaire proposera un planning détaillant les délais de réalisation ainsi que les livrables attendus pour chaque phase du projet.

Les délais indiqués dans l'offre technique du candidat s'appliqueront lors de l'exécution du présent marché.

Figure 10 Ordonnancement souhaité des prestations

5. Description des prestations attendues

Les prestations attendues du présent marché sont décrites dans les paragraphes ci-dessous.

5.1. Prestation 1 : Prise de connaissance et transfert de compétences

5.1.1. Objectif

Cette phase conditionne le bon déroulement des autres prestations. L'objectif du nouveau titulaire est d'être opérationnel et autonome dans les meilleurs délais. Il doit être en mesure de réaliser les prestations demandées dans les meilleures conditions.

5.1.2. Description

Dès le début du marché, une réunion de lancement est organisée, soit 15 jours maximum la notification du marché (voir paragraphe [Préambule](#)), ayant pour objet la présentation des équipes du titulaire, de l'Inserm et de la DGS, ainsi que l'organisation des relations.

A cette occasion, il est remis au titulaire l'ensemble des documents non fournis dans le dossier de consultation et nécessaires au démarrage des prestations.

5.1.2.1 Prise de connaissance

La phase de prise de connaissance ne doit pas durer plus d'un mois.

Durant cette phase et sur demande du titulaire, l'Inserm et le précédent titulaire peuvent organiser des ateliers avec les acteurs concernés pour accompagner le nouveau titulaire dans sa prise de connaissance.

Au titre de cette prestation, le titulaire doit :

- Identifier et mettre en place l'équipe d'intervenants du côté du titulaire pour le marché (selon les termes décrits dans le paragraphe « [Suivi opérationnel des prestations](#) »).
- Prendre connaissance de la documentation spécifique non partagée dans le présent DCE.

5.1.2.2 Transfert de compétences

La phase de transfert de compétences débute à l'issue de la phase de prise de connaissance et ne doit

pas excéder une durée de plus deux mois.

Durant cette phase et sur demande du titulaire, l'Inserm et le précédent titulaire peuvent organiser des ateliers avec les acteurs concernés pour accompagner le titulaire dans sa prise de connaissance.

Cette phase prévoit une durée d'un mois de transition sous la supervision de l'ancien titulaire.

Au titre de cette phase, le titulaire doit :

- Organiser des ateliers avec les parties prenantes pour convenir de certaines modalités pour aider à la montée en compétence.
- Initier les premières instances de comitologie telles que décrites dans le paragraphe « Suivi opérationnel des opérations ».

Le Site CertDc (http://www.CertDc.inserm.fr/accueil_public.php) dispose d'un mode test qui peut être utilisé pendant cette phase pour permettre au titulaire de découvrir l'application web et ses fonctionnalités.

5.1.3. Livrables

- Support et compte-rendu de la réunion de lancement.
- Les supports et comptes rendus de toutes les réunions (ou ateliers) ayant lieu durant cette phase.
- Un rapport de compréhension.
- Une stratégie de déploiement de la solution en prenant en compte les besoins de l'Inserm, de la DGS et des utilisateurs finaux de l'application.
- Le planning prévisionnel livré dans la réponse à l'appel d'offre sera à mettre à jour et à repartager.
- Un document PAQ (Plan d'Assurance Qualité), initié par le titulaire et validé avec l'Inserm et la DGS. Ce document fait apparaître pour chaque document produit les délais accordés pour la relecture des documents par les deux parties, le délai de livraison du document rectifié à la suite des éventuelles remarques de l'Inserm et le délai pour validation. Il entérine également la gouvernance du projet et la comitologie mise en œuvre pour garantir la réussite du projet.

5.2. Prestation 2 : Migration des environnements, applications et des données

5.2.1. Objectif

L'objectif de la phase de migration est d'assurer une transition fluide et sécurisée des applications,

serveurs et données de l'ancien titulaire vers le nouveau titulaire.

Cette migration doit être réalisée de manière sécurisée, en minimisant les interruptions de service et en garantissant l'intégrité et la confidentialité des données.

Le soumissionnaire proposera dans son mémoire technique une stratégie de déploiement détaillée.

5.2.2. Description

Les principales étapes de cette prestation incluent :

1. **Analyse et planification** : Évaluation des systèmes existants, identification des dépendances et élaboration d'un plan de migration et de reprise de contenu détaillé.
2. **Préparation des environnements** : Mise en place des nouveaux environnements d'hébergement et de maintenance, en s'assurant qu'ils répondent aux exigences techniques et de sécurité.
3. **Transfert des données** : Migration des bases de données, des fichiers et des autres éléments de données, en utilisant des méthodes sécurisées pour garantir l'intégrité et la confidentialité. A noter que les certificats en eux même ne seront pas à reprendre lors de la migration. L'essentiel des données à migrer correspondent aux différents référentiels existants, les comptes utilisateurs et administrateurs.
4. **Migration des applications** : Déploiement des applications sur les nouveaux environnements, en effectuant les ajustements nécessaires pour assurer leur bon fonctionnement. L'ensemble de l'infrastructure technique devant être déployée et hébergée par le nouveau titulaire est décrit dans les Dossiers d'architecture techniques qui remis lors du démarrage de la prestation.
5. **Tests et validation** : Réalisation de tests complets pour vérifier que les données et les applications ont été migrées correctement et fonctionnent comme prévu.
6. **Formation et documentation** : Fourniture de la documentation nécessaire et formation des équipes sur les nouveaux environnements et les procédures de maintenance.

Le titulaire doit fournir un rapport détaillé à chaque étape du processus, incluant les résultats des tests et les actions correctives mises en œuvre.

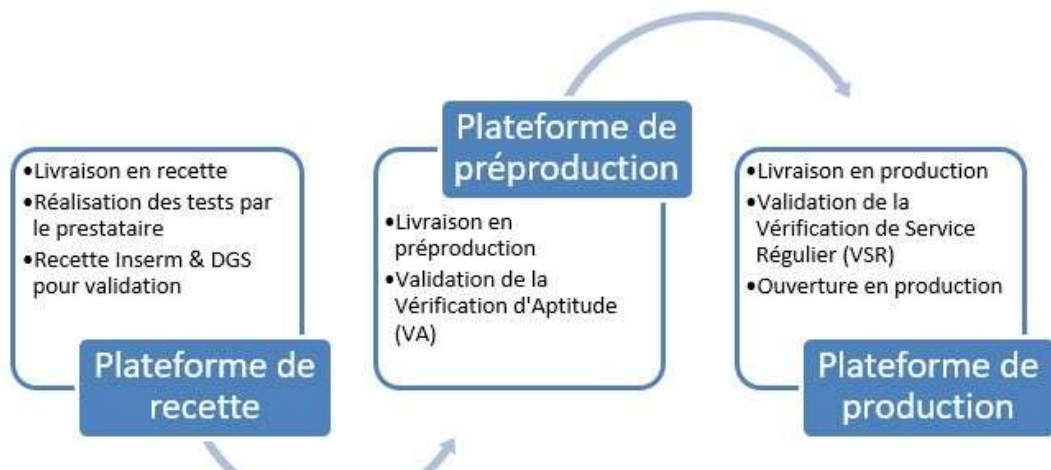


Figure 11 Cycle de livraison

5.2.3. Livrables

Les supports et comptes rendus de toutes les réunions (ou ateliers) ayant lieu durant cette phase :

- Plan de test pour éviter les écueils liés à la reprise des données.
- Résultats des tests.
- Base de données alimentée.
- Procédure de livraison pour chaque phase du cycle de déploiement.
- Les spécifications et DAT/DEX mis à jour si nécessaire.
- Comptes rendus des différents ateliers.
- Nouveau système opérationnel.

5.3. Prestation 3 : Hébergement et exploitation des applications web et mobile de CertDc

Cette partie présente les exigences en termes d'hébergement et d'exploitation des applications web et mobile de CertDc.

Le titulaire s'engage à gérer l'hébergement offrant des garanties de qualité, de coût et de fiabilité selon les besoins détaillés dans les parties suivantes et dans le respect des règles de l'art et des préconisations et recommandations de l'ANSSI.

Tel qu'abordé dans le paragraphe [Respect des normes et standards](#), les recommandations du Référentiel Général de Sécurité, du Règlement Général sur la Protection des Données et la Politique de Sécurité des Systèmes d'Information doivent être respectés.

L'ensemble des infrastructures mises en place par la solution d'hébergement permettent de garantir la disponibilité, la confidentialité, l'intégrité, et la sécurité des données hébergées dans le respect des normes appliquées.

Le titulaire assure la mise en œuvre de ces environnements respectant les spécifications définies au sein du CCTP ainsi que la sécurisation des données et des accès qui y seront implémentés. Il respecte les besoins en performance et stockage définis ci-après.

5.3.1. Dispositions générales d'hébergement

Dans le cadre de cette prestation le titulaire assure la mise à disposition et la prise en charge des environnements suivants :

- Une plateforme de Recette.
- Une plateforme de Préproduction.
- Une plateforme de Production.

En complément de ces 3 environnements attendus par le client, le titulaire pourra déployer des environnements supplémentaires destinés à la réalisation de ses propres activités (ex : développements, tests etc.) auxquels l'INSERM et la DGS n'auront pas accès.

Parmi les 3 environnements préalablement cités, a minima les environnements de Pré-production et de Production doivent être hébergés au sein d'un Cloud privé.

L'Inserm souhaite que l'hébergement soit réalisé en France par un opérateur national et que les données soient hébergées sur plusieurs centres de données (au minimum 2).

Le soumissionnaire précisera dans sa réponse les infrastructures d'hébergement envisagées ainsi que le dimensionnement prévu pour chacun de ces environnements.

5.3.2. Performances

Sur 2024-2025, l'application a connu une fréquentation journalière moyenne de 50 000 connexions.

Il est nécessaire de prévoir une hausse du nombre de connexions et de déclarations dématérialisées sur les prochaines années.

Le système doit ainsi supporter une fréquentation journalière de 60 000 visiteurs uniques et un minimum de 6 000 connexions simultanées (10 % de nombre de visites journalières).

Dans tous les cas l'application doit supporter la charge de 80% de dématérialisation de certification décès (c'est-à-dire plus de 500 000 certificats annuels dématérialisés sur les 650 000 décès signalés en moyenne chaque année).

Le temps de chargement maximal d'une page ne pourra excéder 2 secondes.

5.3.3. Disponibilité et niveaux de service

Le service doit être disponible 7j/7 et 24h/24.

Le temps d'indisponibilité correspond au cumul des temps d'arrêt du service pour :

- La maintenance corrective ou curative comprenant le délai de réponse de l'assistance technique, les temps de diagnostic, d'intervention et de remise en état de fonctionnement.
- La maintenance préventive.
- Les évolutions applicatives.

Le taux d'indisponibilité T est calculé de la manière suivante :

- $T = TI \times 100 / TNO$
- Avec :
 - TI = temps d'indisponibilité hors indisponibilité due à l'Inserm.
 - TNO = temps normalement ouvert.

Le taux d'indisponibilité mensuel ne doit pas excéder 0.5%. Il sera rendu compte des taux d'indisponibilité mensuellement à la personne publique.

En cas d'incident le temps de rétablissement du service exigé (RTO) est de 4h pour une anomalie bloquante et 8h pour une anomalie non bloquante (majeure et mineure).

Il est souhaitable que ce service soit assuré depuis le territoire français.

5.3.4. Sécurité et protection des données

5.3.4.1 Intégrité des données

L'intégrité des données correspond à la prise en charge des quatre éléments suivants : l'intégralité, la précision, l'exactitude/authenticité et la validité.

En cas de perte de données, la perte maximale admissible (RPO) est de 4h. La perte maximale de dossiers acceptable est de 250 certificats par an. Bien évidemment ce seuil ne doit pas être atteint sur un seul mois, une seule journée, une seule région, un seul établissement.

Le titulaire s'engage :

- A assurer que les données hébergées ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.
- A mettre en œuvre les mécanismes qui lui permettront de détecter les altérations et de les réparer.
- A réaliser tous les mois une externalisation des sauvegardes, à les conserver et à les mettre à la disposition sur demande. Toute altération de l'intégrité des données sera considérée comme un incident bloquant.

5.3.4.2 Confidentialité

Les applications CertDc hébergent des données médicales sensibles. La confidentialité des données est donc un enjeu majeur.

Le titulaire s'engage à héberger les données exclusivement en France par un opérateur national assurant un niveau de protection selon les critères de la CNIL.

Le titulaire s'engage à limiter les accès aux données exclusivement en fonction des profils utilisateurs.

Le stockage et le traitement des données devront respecter les normes de sécurité RGPD et RGS suivant le rôle de l'application concernée.

Les données à caractère nominatif hébergées dans le back-office devront être chiffrées.

Le soumissionnaire précisera les moyens mis en place (authentification, chiffrement, cloisonnement etc.) pour se conformer à ces exigences de même que sa façon de traiter un incident lié aux données.

5.3.4.3 Sauvegarde

Le titulaire réalise des sauvegardes selon les modalités suivantes :

- Une sauvegarde quotidienne de l'ensemble des serveurs virtuels.
 - o Sa durée de conservation est de minimum 20 jours.
- Une sauvegarde toutes les 4H de l'ensemble des données chaudes (Certificats de décès).
 - o Sa durée de conservation est de minimum 5 jours. Les données liées aux certificats peuvent être supprimées après expiration de la durée de conservation de la sauvegarde.

Les sauvegardes seront stockées sur plusieurs centres de données (minimum 2), sur des baies dédiées.

La réalisation du processus de sauvegarde par le titulaire n'engendrera aucune interruption de service et sera réalisé de préférence en dehors des heures ouvrées.

Le titulaire s'engage à réaliser des tests de restauration complets tous les semestres a minima.

Le candidat détaillera dans sa réponse la procédure de sauvegarde et restaurant envisagée.

5.3.4.4 Traçabilité

Le titulaire s'engage à assurer une traçabilité totale des actions réalisées par l'ensemble des utilisateurs

du CertDc.

Les actions sensibles ci-dessous doivent être tracées dans des logs et indexées par l'outil de supervision du titulaire :

- Connexion d'un utilisateur en succès.
- Tentatives de connexion d'un utilisateur en erreur.
- Réinitialisation du mot de passe de l'utilisateur.
- Modification du périmètre d'un utilisateur (rôle, équipe, etc...).
- Demandes de rattachement.
- Demandes de raccordement.
- Gestion des certificats (Création / Validation / Rejet / Transmission).

Les logs de traçabilité sont conservés pour une durée de 6 mois.

En cas de non-respect de la traçabilité, un incident de sécurité est ouvert et l'INSERM en est informé.

Le soumissionnaire présentera sa méthodologie et les outils à mettre en œuvre pour conserver et analyser ces traces.

5.3.4.5 Monitoring

Le titulaire a en charge le monitoring, la métrologie et la supervision de l'application CertDc.

Le titulaire assure la supervision de l'ensemble des environnements CertDc et est en mesure de suivre leurs états et leurs performances. Cette supervision peut être assurée par un outil propre au titulaire qui lui permet de disposer de différents indicateurs et d'être alerté en cas de dépassement de seuil.

Le candidat doit pouvoir réaliser les opérations de surveillance ou de maintenance suivantes (liste non-exhaustive):

- Mesure des performances du système (temps de chargement d'une page, nombre de connexions, ...).
- Mesure de la consommation de ressources (espace disque).
- Identification des tentatives d'accès aux données non autorisées.
- Identification des tentatives d'intrusion.
- Identification des tentatives d'export.
- Mesure de la volumétrie des exports réalisées.
- Mesure de la fréquence des exports.

-
- Système de contrôle des modifications de privilèges.

Il revient au titulaire d'être force de proposition au niveau des outils à prévoir pour réaliser ces contrôles.

Le titulaire réalise une synthèse des différents indicateurs suivis qu'il présente lors des COPROJs mensuels organisés tout au long de la durée de validité du marché (voir détails dans le paragraphe [Comitologie](#)).

Le soumissionnaire justifiera dans sa réponse la méthode et les outils mis en place pour répondre à ce besoin.

5.3.5. Audit

Les environnements mis en place par le titulaire doivent être périodiquement contrôlés (fonctionnellement et techniquement) dans le cadre d'audits internes ou externes. L'Inserm pourra à tout moment auditer ou contrôler la sécurité du système CertDc.

Le titulaire s'engage à mettre en œuvre toutes les règles de sécurité nécessaires à la protection informatique de la plateforme dès le développement de celle-ci. Ces règles de sécurité doivent être documentées et L'Inserm pourra vérifier à n'importe quel moment le respect des règles par :

- La réalisation de tests applicatifs et techniques (tentative d'accès à des données non autorisées, tentatives d'intrusion dans le système, etc.).
- La réalisation d'audits (à minima, il est prévu d'auditer la solution avant sa mise en production).
- La vérification des moyens mis en œuvre pour la sécurité.

Le titulaire est tenu de participer tout au long de la prestation à ces actions d'audits. Quelques exemples de sujets à auditer (liste non exhaustive) :

- La base des tickets d'incidents.
- Le code des applications.
- La complétude et la tenue à jour de la documentation (spécifications, consignes d'exploitation, ...).
- Respect du PAQ et des procédures associées.

5.3.6. Evolutivité et maintenance de l'infrastructure technique

Le titulaire s'engage à faire évoluer les outils système (infrastructure, réseaux, serveurs, sécurité système, OS, matériels, VM, Bases de données...) pour maintenir le niveau de sécurité de l'application tout au long du marché.

Ces évolutions du système sont prévues à la prestation du présent marché et ne font pas l'objet de bons

de commande supplémentaires.

Le titulaire doit informer l'INSERM en amont de toute mise à jour majeure, c'est-à-dire susceptible d'impacter la gestion de l'utilisation des applications.

Délai de prévenance attendu :

Mise à jour majeure	30 jours
Mise à jour mineure	7 jours

Des activités pouvant être réalisés au titre de la maintenance de l'infrastructure technique sont, à titre d'exemple :

- Surveillance de l'espace disque, de la mémoire, du CPU.
- Mise à jour des systèmes d'exploitation et des logiciels serveurs.
- Vérification des sauvegardes automatiques.
- Contrôle de la disponibilité.
- Tests de montée en charge ou de bascule.
- Surveillance des certificats SSL, DNS, pare-feu, etc.

Les mises à jour ne doivent pas perturber le fonctionnement du système CertDc.

Le titulaire doit mettre en œuvre les tests nécessaires afin d'éviter toute régression des applications.

Le soumissionnaire détaillera dans sa réponse la méthodologie de déploiement et de mise à niveau (processus de mise en production).

5.3.7. Support technique

Le support technique désigne l'assistance fournie aux utilisateurs ainsi qu'au propriétaire d'un produit ou service numérique (application web, logiciel, site internet, etc.) pour les aider à résoudre des problèmes techniques.

Le support technique demandé répond aux cas d'usage suivants :

- Assistance technique auprès de l'INSERM/DGS, à la suite d'une demande « utilisateur ».
- Assistance technique auprès de l'INSERM/DGS, à la suite d'une demande de l'INSERM/DGS.

La prestation de support technique s'applique sur le périmètre suivant :

- Applications web et mobiles de CertDc.

-
- Ensemble des flux existants et à venir (liste des flux disponible dans le paragraphe [Flux externes de l'application web](#)).

En effet, la prestation de support technique doit notamment permettre de faciliter l'ajout de futurs raccordements des SI et/ou de nouveaux référentiels, pour permettre *in fine* à CertDc de récupérer et transmettre des données. Dans cadre de cette prestation, les établissements de santé dotés de leurs propres outils et souhaitant déployer des interfaces avec CertDc pourront être mise en contact et accompagnés par le titulaire.

Le support technique peut être sollicité par téléphone, mail, ou à la suite d'une demande déposée via l'outil interne de L'INSERM Matrix 42.

L'analyse technique pourra aboutir, soit à la transmission d'une information par le titulaire ; soit à la rédaction déclaration d'une d'anomalie ou d'une demande d'évolution à traiter dans le cadre des prestations 4 et 5.

Livrables :

Dans le cadre du support technique, les livrables suivants sont systématiquement fournis :

- Confirmation de prise en charge du ticket : un accusé de réception précisant le numéro de ticket, le niveau de priorité et le délai estimé de traitement.
- Documentation technique : une synthèse de la demande, des actions réalisées, des solutions apportées ou des recommandations techniques, transmise à la clôture du ticket.

5.4. Prestation 4 : Tierce Maintenance Applicative Corrective et Préventive des applications mobile et Web de CertDc

5.4.1. Objectif

Cette prestation couvre les maintenances corrective et préventive des deux applications CertDc (web et mobile) dans l'objectif de garantir la mise à disposition, pour l'ensemble des utilisateurs, d'une application fonctionnelle, ergonomique et performante.

Cette partie vise à décrire les attendus du pouvoir adjudicateur sur ces types de maintenance afin de garantir à la fois une anticipation et réactivité optimales du titulaire, selon les niveaux d'exigences décrits, et ce afin de limiter l'impact des anomalies dysfonctionnement ou problèmes de stabilité des solutions sur les utilisateurs.

Cette prestation est forfaitaire. La durée de cette prestation est de deux ans, avec la possibilité de la renouveler tacitement deux fois pour une durée d'un an.

La mise en œuvre de la TMA Corrective et préventive des applications CertDc est prévue dès le premier mois de la phase de transfert de compétences et après la prestation de migration (voir [Planning](#)

[prévisionnel](#)).

Cette prestation est suivie par l'équipe projet de l'Inserm lors de comités de maintenance tel que décrit dans le paragraphe [Comitologie](#).

Les spécifications techniques de l'application Mobile sont fournies dans le Dossier d'Architecture technique remis au nouveau titulaire en début de marché.

5.4.2 Maintenance corrective

5.4.2.1 Description de la prestation

La maintenance corrective consiste à corriger les défauts fonctionnels ou techniques de conception, de programmation ou de langage se manifestant par des anomalies de fonctionnement de l'application ou de dégradations, notamment de performance.

La maintenance corrective porte sur des anomalies fonctionnelles et techniques constatées sur les applications mobiles ou web. Elle ne concerne pas les anomalies résiduelles relatives à des évolutions encore en période de VA ou VSR. Ces anomalies seront corrigées au titre de ces périodes.

Les anomalies de type « correctif » sont préalablement saisies dans l'outil de « Ticketing » de l'Inserm : Matrix42.

Afin de garantir une juste désignation des anomalies à figurer dans la charge de maintenance corrective, un traçage de fin des anomalies se fait au moyen de l'outil de « Ticketing » de l'Inserm : Matrix42.

Toute anomalie identifiée ou signalée dans le cadre de la TMA devra être :

- Reproduite en environnement de test.
- Documentée via une fiche d'anomalie.
- Corrigée avec validation via un test de recette.

Un historique des anomalies et des corrections appliquées doit être maintenu.

Au titre de la maintenance corrective, le titulaire devra :

- Analyser et porter un diagnostic fin sur la situation.
- Formaliser l'impact de la solution proposée sur l'application (web ou mobile) en exploitation (conception, architecture des modules, impact sur les postes de travail, mises à jour des documentations).
- Élaborer une solution opérationnelle compatible avec les contraintes des services utilisateurs.

- Présenter un planning de correction conforme aux délais de prise en charge des anomalies.
- Réaliser les tests techniques, unitaires et l'exécution des tests de non-régression (qualification technique du titulaire).
- Effectuer la mise à jour des documentations techniques et fonctionnelles impactées par la correction.

Le titulaire a une obligation de résultat, sans régression de fonctionnement du système d'information et des applications et suivant les délais impartis. La maintenance aboutit à une phase de réception, par l'Inserm, des travaux effectués par le titulaire.

Le processus de prise en charge et de traitement d'une anomalie dans le cadre de la maintenance corrective est présenté dans le schéma et le tableau ci-dessous :

Etape	Intitulé	Description	Responsable
1	Déclaration de l'anomalie	Déclaration de l'anomalie sur Matrix42	INSERM/DGS
2	Qualification du niveau de l'anomalie		INSERM/DGS
3	Prise en charge de l'anomalie	Le titulaire signifie sa prise en charge sur l'outil de ticketing	Titulaire
4	Analyse de l'anomalie et formalisation de la réponse proposée		Titulaire



9	Tests et validation des développements	Tests réalisés par l'INSERM/DGS sur l'environnement de préproduction	INSERM/DGS
---	----------------------------------------	----------------------------------------------------------------------	------------

10	Mise en production	Selon un calendrier précédemment validé avec l'INSERM/DGS	Titulaire
11	Mise à jour de la documentation	Mise à jour de la documentation technique et fonctionnelle	Titulaire

5.4.2.2 Qualification des anomalies

Les anomalies se répartissent suivant le degré de gêne engendré pour l'utilisateur :

- **Anomalie bloquante** : anomalie engendrant l'impossibilité d'utiliser une fonctionnalité nécessaire à l'activité de l'utilisateur.
- **Anomalie majeure** : anomalie non bloquante, mais engendrant une gêne importante dans l'utilisation de l'application.
- **Anomalie mineure** : anomalie non bloquante et non qualifiée de majeure. Il appartient à l'Inserm et la DGS de valider la qualification des anomalies.

5.4.2.3 Délais de prise en charge des constats d'anomalies

Définitions :

- Le **délai de prise en charge** est le temps écoulé entre la **déclaration de l'anomalie** sur l'outil de Ticketing Matrix42 et le **début effectif de son traitement** par l'équipe de maintenance.
- Le **délai de contournement** est le temps écoulé entre la **prise en charge de l'anomalie** et la **mise en place d'une solution temporaire** permettant de **réduire ou éliminer l'impact** sur les utilisateurs, sans corriger définitivement le problème.
- Le **délai de correction** est le temps écoulé entre la **prise en charge de l'anomalie** et la **mise en production de la correction définitive**.

Type d'anomalie	Délai de prise en charge	Délai de contournement	Délai de correction
Bloquante	30 min ouvrées	4 heures ouvrées	1 jour ouvrées
Majeure	2 heures ouvrées	1 jour ouvré	3 jours ouvrés
Mineure	2 heures ouvrées	N/A ou 5 jours ouvrés	10 jours ouvrés

Ces délais s'entendent comme « *délais maximum acceptables* » et s'appliquent aussi bien à l'application Web qu'à l'application mobile.

Les incidents techniques ayant pour origine un partenaire du pouvoir adjudicateur ou du titulaire doivent également être pris en charge par ce dernier, qui coordonne la résolution du problème avec eux.

Toute mise en production doit passer par le cycle : Recette, Préproduction et Production.

Le soumissionnaire précisera dans sa réponse les tarifs qu'il appliquera en cas d'astreinte.

A titre indicatif, sur les 12 derniers mois, 190 incidents ont été signalés dont 4 anomalies bloquantes ; 147 anomalies majeures ; 39 anomalies mineures.

5.4.3 Maintenance préventive

5.4.3.1 Description de la prestation

La maintenance préventive applicative permet de prévenir les dysfonctionnements ou l'obsolescence des applications (code, logique métier, interfaces, composants techniques etc.).

Dans le cadre de cette prestation le titulaire assure sur les activités suivantes durant la période d'exécution du marché :

- Se tenir à jour (veille active) des dernières évolutions des composants techniques externes qui contribuent à la pérennité du fonctionnement de l'application.
- Mener des tests de régression afin de vérifier la cohérence fonctionnelle de l'application.
- Mettre à jour les bibliothèques et frameworks utilisés.
- Contrôler la conformité aux règles métiers.
- Analyser les logs applicatifs pour détecter des comportements anormaux.
- Le cas échéant, proposer soumettre des évolutions réglementaires ou techniques.
- Mettre à jour de la documentation fonctionnelle.

5.4.4 Livrables

- **Rapport de maintenance préventive**
 - Détail des actions réalisées (tests, mises à jour, contrôles).
 - Résultats des vérifications et anomalies détectées.
 - Recommandations éventuelles.
- **Documentation mise à jour**
 - Documentation fonctionnelle et technique actualisée.
 - Historique des modifications.
- **Plan de mise à jour technique**
 - Planning des prochaines actions préventives.

5.5 Prestation 5 : Tierce Maintenance Applicative Evolutive et Adaptative des applications web et mobile de CertDc

La maintenance évolutive vise à adapter l'application à un nouvel environnement technique ou organisationnel tandis que la maintenance adaptative vise à faire évoluer l'application en fonction des nouveaux besoins métiers ou des évolutions technologiques. La maintenance évolutive correspond à toute maintenance, non liée à une anomalie, destinée à intégrer des fonctions complémentaires ou à faire évoluer des fonctions existantes.

Cette prestation se fait par bons de commande.

5.5.1 Objectif

La mise en œuvre de la TMA Evolutive et Adaptative des applications CertDc est prévue après la phase de migration et en parallèle de la fin de la phase « Prise de connaissance et transfert de compétences », tel que présenté dans le paragraphe [Planning prévisionnel](#).

Chaque demande de maintenance évolutive ou adaptative fait l'objet d'un cahier des charges, d'une étude préalable obligatoire et de bons de commandes spécifiques qui seront définis à partir des unités d'œuvres décrites au sein du BPU.

L'Inserm et la DGS feront appel aux ressources et à l'organisation du titulaire pour réaliser des prestations de maintenance évolutive. Selon le nombre et le délai de mise en œuvre des évolutions

demandées, le titulaire doit pouvoir renforcer l'équipe sur le projet d'un commun accord avec l'Inserm et la DGS.

Dans le cadre de ces prestations, le titulaire doit notamment être capable d'assurer les évolutions fonctionnelles ou les adaptations suivantes à la demande de l'Inserm ou de la DGS :

- Ajout ou évolution de fonctionnalités.
- Intégration de migrations techniques au-delà du périmètre des actions de maintenance préventive.

Le titulaire doit également :

- Assister les utilisateurs dans les phases de conception des évolutions et adaptations et dans les phases de recette.
- Effectuer les études d'impact sur l'existant applicatif ainsi que l'estimation (coûts et délais) des travaux à effectuer.
- Mettre à jour les différentes documentations.

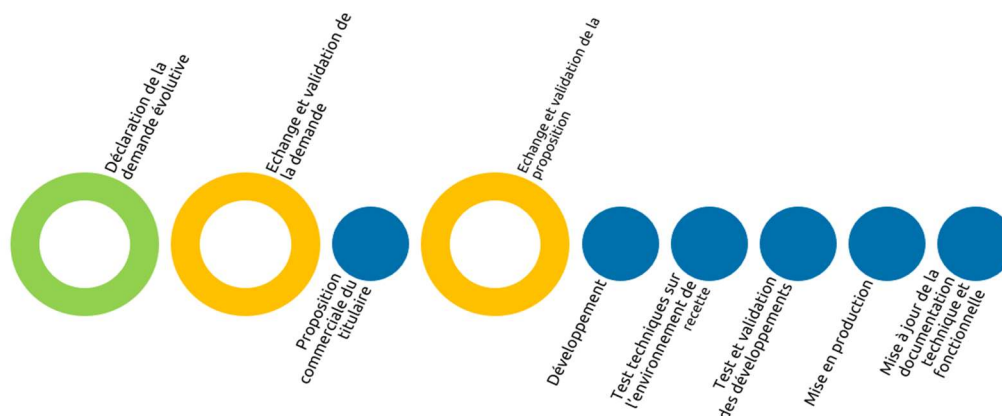
Les délais d'exécution sont précisés dans chaque bon de commande émis et deviennent de facto contractuels.

Cette prestation est suivie par l'équipe projet de l'Inserm lors de comités de maintenance.

La qualité des prestations de TMA doit être une préoccupation constante du titulaire tout au long du cycle de vie du système. C'est pourquoi elle devra être formalisée à travers le Plan d'Assurance Qualité (PAQ).

5.5.2 Modalités de commande et d'exécution des prestations

L'émergence d'un besoin du pouvoir adjudicateur enclenche le processus de suivi de traitement de sa



demande. Le processus de contractualisation à respecter est présenté dans le schéma et le tableau ci-

dessous :

Etape	Intitulé	Description	Responsable
1	Déclaration de la demande d'évolution	Déclaration de la demande évolutive incluant : - expression de besoin - délai de réalisation souhaité La demande est transmise via un document formalisé ainsi que par l'ajout d'un ticket dans Matrix 42 faisant référence au document.	INSERM / DGS
2	Echange et validation de la demande	Validation de la compréhension mutuelle des parties et échanges si nécessaire	INSERM / DGS, Titulaire
3	Proposition commerciale du titulaire	Proposition commerciale du titulaire incluant : - réunions et demandes d'informations complémentaires éventuelles - devis (types et volumes d'UO sollicités) - délai de démarrage et planning de réalisation proposés	Titulaire
4	Echange et validation de la proposition		INSERM / DGS, Titulaire
5	Développement		Titulaire
6	Test techniques sur l'environnement de recette		Titulaire
7	Tests et validation des développements	Tests des développements et validation sur la base de l'expression de besoin	Titulaire
8	Mise en production	Mise en production selon le calendrier validé conjointement	Titulaire
9	Mise à jour de la documentation	Mise à jour de la documentation technique et fonctionnelle	Titulaire

Dans le cadre du suivi de l'exécution du marché, le pouvoir adjudicateur sera vigilant au respect, par le titulaire, des délais de mise en œuvre versus le calendrier initialement demandé.

Le candidat précisera dans sa réponse la méthodologie qu'il propose de mettre en place dans le cadre de la maintenance évolutive ainsi que les dispositions qu'il prévoit afin d'assurer la réactivité de ses équipes et la disponibilité de ses ressources, selon le calendrier attendu.

5.5.3 Livrables

- Les supports et comptes rendus de toutes les réunions (ou ateliers) ayant lieu durant cette phase.
- Le manuel d'installation des évolutions réalisées (modification du code, ajout d'un composant, modification du schéma de la base de données, ...).
- Mise à jour des documents impactés par les évolutions réalisées.
- Rédaction des spécifications détaillées des évolutions demandées.
- L'ensemble du stock de tickets d'évolution suivi et mis à jour.
- Le compte-rendu de la campagne des tests lors de chaque livraison.

5.6 Prestation 6: Réversibilité sortante

5.6.1 Objectif

L'objectif est de permettre à l'Inserm de poursuivre les opérations de TMA et d'hébergement dans des conditions optimales.

Cette prestation a pour but de restituer la connaissance acquise par le titulaire vers les équipes de l'INSERM ou d'un tiers, à la fin du marché, en cas de défaillance du titulaire ou de résiliation du marché.

5.6.2 Description

A la fin de l'exécution du marché et à la demande du pouvoir adjudicateur, le titulaire est tenu, le cas échéant, pendant une durée de 3 mois, de transférer à l'équipe de l'Inserm et la DGS ou toute autre entité indiquée par l'Inserm et la DGS, les informations sur le contexte fonctionnel et technique des applications.

Le titulaire est tenu de mettre à disposition tous les éléments constitutifs de l'écosystème, ainsi que toutes les informations nécessaires et pertinentes pour la bonne prise de connaissance de la nouvelle équipe.

Dans ce cadre, le titulaire doit :

- Lancer la prestation avec les représentants de l'Inserm et de la DGS. Il s'agit d'une réunion destinée à valider le planning et les modalités pratiques de la phase.
- Mettre à disposition tous les éléments faisant l'objet de la maintenance. Il s'agit de préparer un support informatique contenant tous les éléments (programmes, documentations...) gérés par l'équipe et qui seront, à l'issue de cette prestation, placés sous la responsabilité de la nouvelle équipe.

-
- Faire une présentation technique des applications : fourniture d'un état de la configuration technique et présentation de la documentation technique existante. Il s'agit également de présenter, puis de répondre aux questions de la future équipe concernant l'organisation pratique de cette configuration et de cette documentation technique.
 - Faire une présentation détaillée des différents composants et de leurs interdépendances et interconnexions, du code, des workflows existants.
 - Faire une présentation détaillée des données, des fonctionnalités et des traitements spécifiques.
 - Faire une présentation de l'organisation de la maintenance : fourniture d'un état des lieux exhaustif (sujets non clos, constats et demandes de corrections en cours, diffusions en cours et à venir), présentation de l'environnement de développement et d'exploitation (répertoires, installation, procédures mises en œuvre, périodicité et ordonnancement des opérations d'exploitation) et fourniture d'un document décrivant ces divers aspects.
 - Assurer une période de « double supervision » décomposée comme suit :
 - 30 jours ouvrés avec l'Inserm -ou le tiers désigné par l'Inserm-, lors desquels le titulaire sortant reste le pilote à bord et les équipes de l'Inserm assistent la maintenance du système.
 - Suivis de 30 jours ouvrés durant lesquels l'Inserm -ou le tiers désigné par l'Inserm- exécutent et réalisent la maintenance sous le contrôle et le pilotage du titulaire sortant.

Tableau 2 : RACI – Période de double supervision

Phase de réversibilité sortante	Titulaire sortant	Titulaire entrant	INSERM/DGS
Mise à disposition des informations au pouvoir adjudicateur	R	/	A
Prise de connaissance	I, C	R	A
Double supervision – période 1	R	I, C	A
Double supervision – période 2	I, C, A	R	A (sur la validation des attendus de la phase)

Légende RACI

- R = Responsable : Celui qui exécute la tâche.
- A = Autorité / Approbateur : Celui qui valide ou prend les décisions finales.

-
- C = Consulté : Celui dont l'avis est sollicité.
 - I = Informé : Celui qui est tenu informé.

5.6.2.1 Réversibilité du traitement de la TMA

Afin d'assurer la maintenabilité de la plateforme durant cette phase de réversibilité, une période de doubles compétences est également mise en œuvre.

De cette manière, lors de la mise en œuvre de cette prestation, le titulaire sortant titulaire réalise les actions en présence de l'entité qui reprend l'activité afin de le former sur les actions de maintenance et de supervision du système.

Une fois le transfert de compétences assuré, le titulaire sortant supervise les actions réalisées par la nouvelle entité afin de valider leurs livraisons.

5.6.2.2 Réversibilité de l'hébergement

Afin d'assurer la migration de l'hébergement vers la nouvelle architecture, le titulaire fournit les dernières versions du DAT à jour présentant l'ensemble des composants nécessaires pour la reprise des plateformes de Recette, Préproduction et Production.

Il fournit également l'ensemble des documents d'installation et d'exploitation permettant la reprise de l'activité par la future entité.

Le titulaire sortant valide par la suite la bonne mise en œuvre des chacun des trois environnements avant de couper l'ensemble de ses flux et des ces accès à l'application.

5.6.3 Livrables

- Planning organisationnel des présentations et formations ;
- Les documentations relatives aux composants logiciels et données.
- Toutes les documentations de l'application.
- Livraison finale de tous les éléments faisant l'objet de la maintenance rappelés dans les différentes sections du présent document.

6 Suivi opérationnel des prestations

6.1 Description

Durant l'ensemble du marché, un suivi opérationnel est nécessaire pour la bonne conduite du projet.

Le titulaire désigne un contact unique (Chef de projet) qui est l'interlocuteur privilégié pour l'Inserm et la DGS afin d'obtenir un suivi et un état d'avancement tout au long du projet.

Un ensemble de documentation et une comitologie seront validés lors de la réunion de lancement permettant ainsi de préciser les modalités pratiques.

Afin de suivre l'avancement des tickets et demandes d'évolution, des comités de suivi hebdomadaires sont organisés pour établir le bilan des actions réalisées et celles planifiées pour la semaine à venir. Ce comité a pour objectif de veiller au bon déroulement des opérations et de prendre toutes les décisions utiles. Elle est composée de représentants du titulaire, de l'Inserm, de la DGS et des acteurs jugés nécessaires.

Des comités de pilotage mensuels sont organisés entre l'Inserm, la DGS et le titulaire. Ces comités permettent de préciser le taux d'avancement et les difficultés rencontrées ainsi que d'identifier des solutions aux potentiels points de blocage.

Le projet se terminera par une réunion de clôture permettant la validation et la bonne réalisation de la prestation.

Par ailleurs, l'Inserm peut organiser certains comités de suivi qui réunissent le titulaire et d'autres directions selon des besoins ponctuels.

6.2 Comitologie

Comité	Objectif	Fréquence	Participants
COPIL (Comité de pilotage)	Valider les orientations, prioriser les évolutions	Trimestriel	Directeur projet, direction titulaire, MOA, AMOA, Responsable TMA
COPROJ (Comité de projet)	Suivi opérationnel, respect du planning, suivi des charges	Mensuel	Chef de projet TMA, AMOA, MOE

COTECH (Comité Technique)	Suivi technique, analyse des incidents, validation des correctifs et évolutions	Hebdomadaire	Chef de projet TMA, AMOA, MOE
---------------------------	---------------------------------------------------------------------------------	--------------	-------------------------------

6.3 Dispositif humain

Comme évoqué précédemment, le titulaire désigne un contact unique (Chef de projet) qui est l'interlocuteur privilégié pour l'Inserm et la DGS afin d'obtenir un suivi et un état d'avancement tout au long du projet.

Le candidat communiquera dans sa réponse le dispositif envisagé pour les prestations : organisation, effectifs (dédiés ou non), profils des membres. Il justifiera de la pertinence du dispositif proposé et de son adéquation aux besoins du présent marché.

6.4 Livrables

- Ordre du jour, supports et comptes rendus de comités.
- Planning détaillé à jour.
- Document de suivi des risques.
- Tableau de bord de suivi des livrables.
- Bilan projet.
- Tout autres documents nécessaires à la gestion du projet qui seront précisés dans le PAQ.

7 Modalités pratiques de la prestation

7.1 Horaires et disponibilité du titulaire

L'ensemble des prestations doit être réalisé sur une plage horaire minimale s'étalant de 8h à 18h, du lundi au vendredi.

Le candidat pourra proposer une plage horaire plus étendue sur une ou l'ensemble des prestations (support technique, hotline, TMA etc.), dans ce cas, il détaillera ce point dans sa réponse.

Il est entendu que les délais d'intervention de la prestation de TMA, décrits dans le paragraphe [Délais de prise en charge des constats d'anomalies](#), s'inscrivent dans la plage horaire appliquée par le titulaire.

7.2 Langues

Les réponses à l'appel d'offre, les documents et livrables seront produits en français.

7.3 Changement du périmètre

Aucun changement du périmètre du projet ne peut être apporté en cours d'exécution sans l'autorisation écrite de l'Inserm. Les frais résultant de changements non autorisés et toutes leurs conséquences ainsi que tout le travail supplémentaire exécuté sans ordre écrit sont à la charge du titulaire.

Néanmoins, en cours du projet, l'Inserm peut demander au titulaire de réaliser d'éventuels changements sur le périmètre du projet (tels que demandes d'évolution, contraintes réglementaires...). Le titulaire étudiera ces changements, leurs impacts et proposera une étude financière pour leur réalisation.

8 Annexes

- Cadre de réponse technique