

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(C.C.T.P)

REFERENCE ACCORD-CADRE : UCANSS_26/AC/17

FOURNITURE DE CERTIFICATS DE SIGNATURES ET DE CACHETS ELECTRONIQUES POUR LES
ORGANISMES DE SECURITE SOCIALE

SOMMAIRE

1. OBJET DE L'ACCORD-CADRE	4
2. PRESENTATION.....	4
3. PRÉSENTATION DES ORGANISMES BÉNÉFICIAIRES DE L'ACCORD-CADRE.....	5
4. LE CONTEXTE RÉGLEMENTAIRE, FONCTIONNEL ET TECHNIQUE, SES CONSEQUENCES	11
4.1 Les textes applicables	11
4.2 Conformité et niveaux de signature eIDAS.....	11
4.3 Tiers de confiance et autorité de certification	12
4.4 L'environnement fonctionnel et technique existant	12
4.5 La conformité aux politiques SSI des branches.....	13
4.6 Sécurité des données et traçabilité	15
4.7 Règlement général sur la protection des données (RGPD).....	16
5. LES PRESTATIONS ATTENDUES.....	16
5.1 Gestion du projet	16
5.2 POC éventuels, livraison des certificats et cachets et mise en service.....	16
5.2.1 POC (Proof of concept) éventuels.....	16
5.2.2 Commande.....	16
5.2.3 Délivrance, livraison et accompagnement à l'usage	17
5.3 Installation des certificats de signature et cachets électroniques sur les postes de travail et mobiles	17
5.3.1 Prérequis techniques	17
5.3.2 Pilote d'installation et assistance au démarrage.....	17
5.3.3 Délais	17
5.4 Assistance à l'utilisation et gestion des incidents.....	17
5.4.1 Support d'assistance technique aux utilisateurs	17
5.4.2 Gestion des incidents remontés par les utilisateurs	18
5.5 Maintenance	18
5.5.1 Maintenance corrective	18
5.5.2 Évolution technique ou réglementaire	18
5.6 Renouvellement et révocation	19

5.6.1 Renouveaulement	19
5.6.2 Révocation.....	19
5.7 Pilotage et Comitologie.....	19
5.8 Accompagnement, Formation et conduite du changement.....	20
6 SYNTHÈSE	22

1. OBJET DE L'ACCORD-CADRE

Le présent accord-cadre a pour objet de répondre aux besoins de dématérialisation des circuits de signature dans les organismes de Sécurité sociale.

Cet accord-cadre est interbranche et inter-régimes, tous les organismes de la Sécurité sociale peuvent en être bénéficiaires, à savoir les Caisses Nationales, Centrale, ainsi que tous les organismes locaux.

L'accord-cadre est multi-attributaires (deux titulaires maximums, sous réserve d'un nombre suffisant de candidats).

Périmètre des prestations

L'accord-cadre porte exclusivement sur la fourniture de certificats de signature électronique pour personnes physiques et de certificats de cachet électronique pour personnes morales, conformes au règlement eIDAS, aux quatre niveaux de signature et de cachet électroniques, sur support cryptographique (clé USB ou équivalent) ou à distance (cf. PSE n°1 à 4 du Bordereau des prix), ainsi que sur les prestations associées (commande, délivrance, support, maintenance, renouvellement, révocation).

Ne sont pas inclus dans le périmètre : la fourniture d'un parapheur électronique, ainsi que la fourniture d'applicatifs de signature ou de cachet déployés sur les SI des organismes.

Chaque organisme de Sécurité sociale pourra solliciter la mise à disposition des prestations par bons de commande. L'UCANSS, en tant que pouvoir adjudicateur, conduit et conclut cet accord-cadre.

2. PRESENTATION

Le présent Cahier des charges a pour objet de définir les conditions de fourniture de certificats de signatures électroniques pour signer électroniquement les documents et de cachets électroniques pour sceller des documents.

Le titulaire sera en mesure de répondre à minima à toutes les spécifications listées. Les organismes solliciteront ce dont ils ont besoin par bon de commande auprès du titulaire.

Objectif :

- ✓ Permettre aux Caisses Nationales, Centrale et organismes locaux de disposer de certificats de signature électronique pour personnes physiques et de certificats de cachet électronique pour personnes morales, conformes au règlement eIDAS, aux quatre (4) niveaux de signature et de cachet, sur support cryptographique ou à distance.

3. PRÉSENTATION DES ORGANISMES BÉNÉFICIAIRES DE L'ACCORD-CADRE

En tant que centrale d'achat, l'UCANSS conclut ce marché pour le compte de l'ensemble des organismes de la Sécurité sociale en France métropolitaine, Corse comprise, et dans les DOM.

La Sécurité sociale se compose de 7 branches :



Les organismes bénéficiaires de ce marché sont ceux visés à l'article L. 224-5 du Code de la Sécurité sociale. Il s'agit notamment des organismes suivants :

A noter, les ARS ne font pas partie du périmètre de ce marché.

▪ L'UCANSS

L'UCANSS est un organisme de droit privé chargé d'une mission de service public. Elle a un effectif de 240 agents et son siège social est implanté, pour la majeure partie de ses activités, au 6 rue Elsa TRIOLET, 93100 MONTREUIL.

Ses missions sur le plan national sont essentiellement :

- De traiter les questions se rapportant aux conditions de travail, de rémunération et d'emploi du personnel des organismes de Sécurité sociale ;
- D'instruire sur le plan technique les dossiers concernant les opérations immobilières des organismes ;
- D'organiser et de coordonner la formation professionnelle et le perfectionnement du personnel des organismes de Sécurité sociale ;

- D'assurer la fonction de centrale d'achat pour les organismes de la Sécurité sociale en application de l'article L. 224-5 du code de la sécurité sociale, des articles L. 2113-2 du Code de la commande publique et de l'article 20 de l'arrêté du 19 juillet 2018 portant réglementation sur les marchés publics des organismes de Sécurité sociale.

Des informations complémentaires sont accessibles sur le portail de l'UCANSS : <http://www.ucanss.fr>

▪ La Branche Maladie

L'Assurance Maladie du Régime général de Sécurité sociale est le principal assureur obligatoire de la santé des Français ; couvrant 4 personnes sur 5 contre les risques maladie, maternité, invalidité, accidents du travail, maladies professionnelles et décès.

Pour répondre, dans les contraintes fixées, aux attentes dont elle fait l'objet dans le cadre de ces missions et objectifs, selon les moyens fixés, l'Assurance Maladie s'est organisée en un réseau structuré autour de 3 dimensions géographiques décrites ci-dessous. La liste des organismes bénéficiaires du marché sont les suivants :

L'échelon national comprend :

1. La Caisse Nationale d'Assurance Maladie en tant qu'Établissement Public (CNAM) « autonome », tête du réseau de la Branche Maladie chargée de définir les politiques de gestion du risque et de piloter le réseau d'organismes chargés de les mettre en œuvre ;
2. 11 centres informatiques rattachés à la CNAM disposant de missions spécifiques sur le Système d'information national : certains sont spécialisés en Centres de services métiers ; d'autres en Centres de services techniques ;
3. 16 Directions Régionales du Service Médical (DRSM), rattachées à la CNAM chargées d'accompagner et de contrôler les assurés et professionnels de santé.

L'échelon régional comprend :

1. La CRAMIF ayant des missions relevant de la branche Maladie ;
2. Le Groupe UGECAM qui propose une offre de soins et d'accompagnement médico-social, adaptée aux besoins des populations. Les missions des établissements du Groupe UGECAM sont nombreuses : soigner et rééduquer toute personne en perte d'autonomie ou en situation de handicap, quel que soit son âge, et développer des programmes de réinsertion dans la vie dite ordinaire, dont la réinsertion professionnelle.
Avec plus d'1.3 milliard de chiffre d'affaires, le Groupe UGECAM est un opérateur majeur de santé privé non lucratif, particulièrement présent dans les domaines des soins de suite et de réadaptation (10% de l'offre nationale en rééducation fonctionnelle, 5% des soins de suite) et le secteur médico-social (26% de la réinsertion professionnelle des travailleurs handicapés).
Le Groupe UGECAM compte 249 établissements et services sanitaires et médico-sociaux, 15 986 lits et places et 14 350 salariés.

<https://www.groupe-ugecam.fr/le-groupe-ugecam>

Les entités locales sont représentées au travers de :

1. 101 Caisses Primaires d'Assurance Maladie (CPAM) et 1 Caisse Commune de Sécurité Sociale (CCSS Mende- regroupant toutes les branches de la Sécurité Sociale pour le département de la Lozère), disposant pour certaines de centres de santé, de centres dentaires et de centres d'exams de santé.

Chaque CPAM gestionnaire est juridiquement responsable de son centre de santé, de son centre d'examen dentaires. Les CPAM passent les commandes pour leur compte.

2. 2 Unions de Caisses : l'UC CMP et l'UC IRSA, organismes du régime général sur le champ de la prévention avec pour mission principale l'offre d'examen de prévention en santé.
3. 5 Caisses Générales de Sécurité Sociale (CGSS) regroupant les services de l'Assurance Maladie, de l'Assurance Retraite, de l'Union de Recouvrement des cotisations de Sécurité Sociale et d'Allocations Familiales (URSSAF) et du régime Agricole (MSA) dans les départements d'Outre-Mer. La CGSS de la Guadeloupe dispose d'un centre d'examen de santé qui lui est juridiquement rattaché.

Une Caisse équivalente (assurant les prestations de toutes les autres branches de la sécurité sociale, allocations familiales, régime agricole et des indépendants...) existe pour Mayotte.

Des informations complémentaires sont accessibles sur le site de l'assurance maladie :

<https://www.assurance-maladie.ameli.fr>

▪ La Branche retraite

Le champ d'application de la prestation porte sur les personnels de la branche retraite Caisse Nationale d'Assurance Vieillesse (CNAV) et son réseau constitué de 15 Carsat.

La Branche Retraite du régime général de la Sécurité sociale gère la retraite de base des salariés du commerce, de l'industrie, des services et des travailleurs indépendants.

L'Assurance Retraite développe une politique d'action sociale axée sur la prévention de la perte d'autonomie et l'accompagnement des personnes socialement fragilisées.

Elle est composée de :

- La Caisse Nationale d'Assurance Vieillesse (CNAV) qui est un établissement public administratif sous la tutelle de l'Etat ;
- 15 CARSAT, organismes régionaux (Caisse d'Assurance Retraite et de la Santé au Travail) en métropole.

Plus d'informations : <http://www.lassurance retraite.fr>

▪ La Branche Famille

Les prestations familiales composent la "branche Famille" de la Sécurité sociale, à travers le réseau constitué par la Caisse nationale des Allocations familiales (CNAF) et l'ensemble des caisses d'Allocations familiales (Caf) et autres organismes communs avec plus de 30 000 salariés.

Les 101 Caisses d'Allocations Familiales sont des organismes de droit privé chargés d'une mission de service public.

Les 9 sites informatiques intégrés dans une direction générale déléguée aux SI assurent la fourniture et la maintenance. Ces 9 sites sont répartis sur tout l'hexagone (Lyon, Metz, Dijon, Caen, Rennes, Sophia-Antipolis, Le Mans, Montreuil, Noisy le Grand).

Des informations complémentaires sont accessibles sur le site de la CNAF : <http://www.caf.fr>

▪ **La Branche Recouvrement**

L'Urssaf Caisse nationale est la caisse nationale de la branche du Recouvrement.

Établissement public à caractère administratif sous tutelle de l'Etat, l'Urssaf Caisse nationale oriente et anime les politiques de recouvrement et de contrôle, gère la trésorerie du Régime Général, conçoit les services de simplification offerts aux usagers, organise et alloue les moyens des organismes du recouvrement, produit des statistiques socio-économiques à destination de ses partenaires et des pouvoirs publics.

Le réseau du recouvrement social regroupe depuis le 1er janvier 2022, 21 Urssaf régionales sur le territoire métropolitain et 4 CGSS dans les départements d'Outre-mer.

Il s'agit d'organismes de droit privé qui assurent le service public du recouvrement, c'est-à-dire qu'ils procèdent à la collecte des cotisations et contributions sociales auprès des employeurs et cotisants de leurs circonscriptions.

L'effectif de la branche Recouvrement au 1er janvier 2022 est de 15 106 salariés.

Des informations complémentaires sont accessibles sur le portail du recouvrement : <http://www.urssaf.fr>

▪ **La Branche autonomie (CNSA)**

La Caisse Nationale de solidarité pour l'autonomie (CNSA) est un établissement public national à caractère administratif, créé par la loi du 30 juin 2004, jouissant de la personnalité morale et de l'autonomie financière qui, depuis le 1er janvier 2021, est gestionnaire de la 5e branche de la Sécurité sociale, la branche Autonomie.

Les nouvelles missions de la CNSA sont définies dans l'article 32 de la loi de financement de la Sécurité sociale pour 2021 :

- Veiller à l'équilibre financier de cette branche. À ce titre, elle établit les comptes de celle-ci et effectue le règlement et la comptabilisation de toute opération relevant de cette branche. Elle est chargée de la gestion du risque ;
- Piloter et assurer l'animation et la coordination, dans le champ des politiques de soutien à l'autonomie des personnes âgées et des personnes handicapées, des acteurs participant à leur mise en œuvre en vue de garantir l'équité, notamment territoriale, la qualité et l'efficacité de l'accompagnement des publics concernés ;
- Contribuer, en assurant une répartition équitable sur le territoire national, au financement et au pilotage :
 - D'une politique de prévention de la perte d'autonomie et de lutte contre l'isolement ;
 - Des établissements et services sociaux et médico-sociaux ;
 - Des prestations individuelles d'aide à l'autonomie et des dispositifs mis en place aux niveaux national ou local en faveur de l'autonomie et des proches aidants ;
 - Et de contribuer au financement de l'investissement dans le champ du soutien à l'autonomie.

- Contribuer à l'information des personnes âgées, des personnes handicapées et de leurs proches aidants, notamment en créant des services numériques et en favorisant la mise en place de guichets uniques au niveau départemental permettant de faciliter leurs démarches administratives et le suivi personnalisé de leurs parcours ;
- Contribuer à la recherche et à l'innovation dans le champ du soutien à l'autonomie des personnes âgées et des personnes handicapées ;
- Contribuer à la réflexion prospective sur les politiques de l'autonomie, leurs possibles adaptations territoriales et de proposer toute mesure visant à améliorer la couverture du risque, en prenant notamment en considération les inégalités liées au sexe afin d'élaborer des mesures correctives ;
- Contribuer à l'attractivité des métiers participant à l'accompagnement et au soutien à l'autonomie des personnes âgées et des personnes handicapées, notamment au travers de ses actions en faveur de la formation et de la professionnalisation des professionnels.

Des informations complémentaires sont accessibles sur le portail : <https://www.cnsa.fr>

▪ **La Mutualité Sociale Agricole (MSA)**

La MSA assure la couverture sociale de l'ensemble de la population agricole et des ayants-droits : exploitants, salariés (d'exploitations, d'entreprises, de coopératives et d'organismes professionnels agricoles), employeurs de main d'œuvre, à travers un réseau formé par :

- Une Caisse centrale de la MSA (CCMSA), un organisme de droit privé chargé d'une mission de service public ;
- 35 caisses pluri-départementales ou régionales réparties sur le territoire métropolitain.

Des informations complémentaires sont accessibles sur le portail <http://www.msa.fr/>

▪ **La Branche Filieris (CANSSM)**

La Caisse autonome nationale de la sécurité sociale dans les mines (CANSSM) est l'organisme gestionnaire du régime spécial de la sécurité sociale dans les mines. Elle a été créée par le décret n° 46-2769 du 27 novembre 1946 modifié portant organisation de la sécurité sociale dans les mines.

La CANSSM gère l'offre de santé Filieris qui délivre des soins et de l'accompagnement dans les territoires où elle est présente.

La CANSSM - Filieris est placée sous la tutelle du Ministère du Travail, de la Santé et des solidarités et du ministère de l'Économie et des Finances et de la Souveraineté industrielle et numérique.

La Caisse autonome nationale est administrée par un conseil d'administration dont les administrateurs représentent les exploitants et anciens exploitants, les affiliés, l'Etat, la CNAM et des personnalités qualifiées.

La CANSSM - Filieris est constituée d'un seul organisme : le siège est basé à Paris et les trois services territoriaux, également appelés Directions régionales (DR), sont situés à Lens pour la DR du NORD, à Metz pour la DR de l'EST, à Alès pour la DR du SUD.

La gestion des activités de prestations de sécurité sociale a été progressivement déléguée à d'autres organismes : Caisse des dépôts et consignations (CDC) pour l'assurance vieillesse et invalidité, Caisse nationale d'assurance maladie (CNAM) pour l'assurance maladie, maternité, accidents du travail et maladies professionnelles. La CANSSM reste garante du respect des droits des affiliés en application des règles propres au régime minier et de la qualité du service rendu aux assurés.

L'offre de santé Filieris est composée au 1er janvier 2024 de :

- 130 centres de santé (avec antennes), dont 110 centres de santé polyvalents principaux (pouvant comprendre plusieurs activités : médecine spécialisée, générale, soins infirmiers, kinésithérapie, dentaire) et 13 antennes et 7 centres de santé dentaires
- 22 établissements sanitaires et médico-sociaux
- 11 établissements de soins médicaux et réadaptation intégrant 3 unités de soins de longue durée (USLD)
- 11 établissements médico-sociaux dont 6 EHPAD
- 16 services autonomie à domicile - Soins (services de soins infirmiers à domicile - SSIAD)
- 2 services autonomie à domicile - Accompagnement (services d'aide et d'accompagnement à domicile - SAAD)
- 14 pharmacies
- 1 centre d'optique
- 1 service de matériel médical
- 1 centre de vaccination
- 1 centre d'examens de santé
- 1 centre gratuit d'information, de dépistage et de diagnostic (CeGIDD)
- 1 maison des aidants

L'entité FILIERIS comporte 4500 collaborateurs.

Les autres régimes de Sécurité sociale sont notamment :

CAVIMAC : Caisse d'Assurance Vieillesse Invalidité et Maladie des Cultes

CAVP (PHARMACIENS) : Caisse d'Assurance Vieillesse des Pharmaciens

CNBF (BARREAUX FRANCAIS) : Caisse Nationale des Barreaux Français

CAMIEG : Caisse d'assurance maladie des industries électriques et gazières

CNIEG : Caisse Nationale des Industries Electriques et Gazières

CNMSS : Caisse Nationale Militaire de Sécurité Sociale

CPRPSNCF : Caisse de Prévoyance et de Retraite du personnel de la SNCF

CRPCEN : Caisse de Retraite et de Prévoyance des Clercs et Employés de Notaires

CRPRATP : Caisse de Retraites du Personnel de la Régie autonome des transports parisiens

NB : d'autres organismes de la Sécurité sociale pourront adhérer à ce marché.
--

4. LE CONTEXTE RÉGLEMENTAIRE, FONCTIONNEL ET TECHNIQUE, SES CONSÉQUENCES

4.1 Les textes applicables

- Règlement eIDAS n°910/2014 du 23 juillet 2014 - Essentiellement consacré à l'identification électronique et aux services de confiance ;
- L'application du règlement par l'ANSSI et la liste des prestataires de services de confiance dont les produits et services sont conformes au règlement eIDAS :
 - Une attention particulière sera portée aux données personnelles demandées qui devront être parfaitement en adéquation avec l'usage du logiciel,
 - Le logiciel doit posséder une fonction d'anonymisation des données, pour les fins statistiques,
 - Le titulaire devra respecter le droit à l'information dans sa totalité ;
 - Le titulaire devra respecter le référentiel d'exigences de l'ANSSI applicable à un prestataire de services informatiques en nuage (SecNumCloud v3.2) ;
- Les normes européennes de l'ETSI ;
- L'Annexe 12 du Code de la commande publique : Arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique.

4.2 Conformité et niveaux de signature eIDAS

Les certificats de signature et de cachets électroniques doivent être conformes au règlement eIDAS en garantissant :

- Pour les certificats de signature électronique, l'intégrité du document signé et permettant d'identifier son signataire ;
- Pour le cachet électronique, l'intégrité et l'origine du document.

Afin de pouvoir signer toutes typologies de documents, le titulaire devra répondre aux 4 niveaux de signature électronique du règlement eIDAS, à savoir :

- La signature électronique simple ;
- La signature électronique avancée ;
- La signature électronique avancée avec certificat qualifié ;
- La signature électronique qualifiée.

Les mêmes 4 niveaux sont attendus pour les cachets électroniques « personne morale ».

Les produits doivent faire partie de la liste nationale de confiance des produits et services qualifiés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations).

Les normes de signature ETSI doivent également être respectées.

4.3 Tiers de confiance et autorité de certification

Le titulaire doit être qualifié eIDAS (prestataire de services de confiance qualifié – PSCQ) et s'appuyer sur une Autorité de Certification conforme eIDAS/ETSI et démontrer une maîtrise opérationnelle de la chaîne de confiance.

4.4 L'environnement fonctionnel et technique existant

Applications métier

Les organismes comptent des applications dédiées à l'activité des différentes branches et des applications dont l'usage est transverse.

Chaque organisme est autonome dans la gestion de son système informatique.

Périmètre documentaire

Les documents à signer et/ou sceller électroniquement peuvent être de diverses natures :

- Contrats et conventions de formation *;
- Contrats de travail ;
- Conventions ;
- Marchés publics ;
- Actes administratifs ;
- Validation de flux financier DCF ;
- Bons de commande ;
- Éléments de paie ;
- Etc.

L'objectif est de généraliser la signature électronique et/ou le cachet électronique en tenant compte du niveau de signature ou de cachet requis par rapport aux risques et préjudices encourus.

Conditions d'intégration aux SI des organismes

Aucun composant logiciel propriétaire du titulaire n'est installé sur les systèmes d'information des organismes (postes de travail, serveurs, applicatifs métier), à l'exception des pilotes nécessaires à l'utilisation d'un support cryptographique.

Pour les certificats à distance (PSE n°1 à 4), les certificats sont hébergés par le titulaire dans son infrastructure conforme aux exigences eIDAS et ETSI applicables à son niveau de qualification. Leur utilisation par les organismes s'effectue via les parapheurs compatibles ou via une interface mise à disposition par le titulaire, sans intégration spécifique requise sur les SI des organismes.

Les modalités techniques d'accès au service de signature à distance sont précisées dans la réponse technique du candidat (cf. cadre de réponse technique).

Cas de la branche Famille

Pour les conventions de financement et de partenariat, les avenants associés et les notifications de décision relevant du champ de l'action sociale, les certificats fournis doivent être utilisables au sein des applicatifs métier de la branche Famille dans les mêmes conditions de non-installation logicielle énoncées ci-dessus.

Exclusions expresses du périmètre du marché pour la branche Famille :

Sont exclus expressément du champ du présent marché, le recours à des signatures pour signer des conventions de financement et partenariats, leurs avenants, ainsi que les notifications de décision relevant aussi du financement et du partenariat.

Postes de travail et serveurs

Environnements Windows 10 et 11, navigateurs Edge, Firefox, Chrome.

Parapheurs

Les certificats fournis doivent être compatibles avec les principaux parapheurs électroniques utilisés par les organismes de Sécurité sociale. Le titulaire indique dans son offre, et maintient à jour pendant toute la durée de l'accord-cadre, la liste des parapheurs avec lesquels la compatibilité est établie.

4.5 La conformité aux politiques SSI des branches

Politique de Sécurité des Systèmes d'Information (PSSI)

Afin de garantir la protection des données sociales sensibles, le titulaire se conforme à la Politique de Sécurité des Systèmes d'Information (PSSI) applicable à chaque branche bénéficiaire, telle que transmise en annexe du présent CCTP (PSSI de la branche famille) ou lors de l'adhésion de l'organisme au marché.

Plan d'Assurance Sécurité (PAS) pour tous les organismes bénéficiaires sauf branche Maladie

Le titulaire doit disposer d'un Plan d'Assurance Sécurité (PAS) couvrant l'ensemble des systèmes d'information mis à disposition du pouvoir adjudicateur, notamment le portail de commande en ligne.

Ce document doit être transmis au pouvoir adjudicateur lors de la remise de son offre, puis mis à jour à chaque évolution significative du système.

Le portail de commande doit faire l'objet d'audits de sécurité réguliers, réalisés par un prestataire tiers qualifié (de préférence certifié PASSI – Prestataire d'Audit de la Sécurité des Systèmes d'Information).

Les rapports de synthèse de ces audits, ainsi que les plans de remédiation associés, doivent être communicables sur demande du pouvoir adjudicateur.

Le titulaire s'engage à respecter les exigences de sécurité applicables aux Prestataires de Services de Confiance (PSC) telles que définies par le règlement eIDAS et les politiques de certification applicables, notamment en ce qui concerne :

- La confidentialité et l'intégrité des données transmises via le portail ;
- La gestion des accès et authentification des utilisateurs (authentification forte recommandée).

Tout incident de sécurité affectant le portail de commande doit être notifié au pouvoir adjudicateur conformément aux obligations du RGPD et aux bonnes pratiques ANSSI.

Plan d'Assurance Sécurité (PAS) spécifique à la branche Maladie

A- Obligation du Titulaire

Le Titulaire s'engage formellement à respecter les exigences de sécurité du PAS Cnam et celles de ce présent CCTP. Il devra exécuter l'ensemble de ses obligations de résultats et de moyens tout au long de l'accord-cadre.

Conformément au RGPD, le Titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art en vue d'optimiser la protection des données et éviter les risques ci-dessus.

En particulier, il s'engage à informer la Cnam des risques d'une opération envisagée, des incidents éventuels ou potentiels et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Le Titulaire informera préalablement la Cnam de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du service, la dégradation d'intégrité et/ou de confidentialité des données.

Le Titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations. Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans son système d'information, l'évolution des technologies et des capacités d'attaques doivent être prises en compte.

B-Démarche du Plan d'Assurance Sécurité

"Le PAS en annexe [Annexe - Exemple-PAS type Cnam *] comprend l'ensemble des exigences de sécurité liées à l'environnement du Titulaire utilisés dans le cadre du marché.

En début de marché lors de la phase d'initialisation, le Titulaire devra rédiger le PAS et élaborer les dispositifs de sécurité afférents pour démontrer le respect des exigences de sécurité stipulées par la Cnam.

Tout au long du marché :

- Les dispositifs de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques doivent être pris en compte.

- le Titulaire devra réaliser l'auto-évaluation de conformité aux exigences de sécurité stipulées par la Cnam et suivre les indicateurs de sécurité. Il s'engage à informer la Cnam des risques, des incidents et de proposition de mise en conformité ayant trait à la sécurité.

- Le PAS pourra faire l'objet d'évolution dont les modalités sont précisées dans le document lui-même, le titulaire s'engage à mettre à jour le PAS conformément aux directives de la Cnam

4.6 Sécurité des données et traçabilité

Sécurité de l'infrastructure du titulaire

Le titulaire est responsable de la sécurité de son infrastructure de délivrance des certificats et, le cas échéant, d'hébergement des certificats à distance. Il met en œuvre, et maintient pendant toute la durée de l'accord-cadre, les dispositions de sécurité conformes aux exigences du règlement eIDAS, aux normes ETSI applicables et aux référentiels d'exigences de l'ANSSI applicables aux prestataires de services de confiance qualifiés.

Traçabilité et journalisation

Le titulaire assure la journalisation horodatée et inaltérable de l'ensemble des opérations relatives au cycle de vie des certificats émis dans le cadre de l'accord-cadre, notamment les opérations d'enregistrement, d'émission, de renouvellement, de suspension, de révocation et, pour les certificats à distance (PSE n°1 à 4), les appels au service de signature ou de cachet.

Conservation des données d'enregistrement et des journaux

Le titulaire conserve les données d'enregistrement des porteurs et responsables de cachet, ainsi que les journaux d'opérations, dans des conditions et pour des durées conformes à sa politique de certification, aux exigences eIDAS et aux référentiels d'exigences de l'ANSSI applicables à son niveau de qualification. Les données d'enregistrement et les journaux sont conservés dans des conditions garantissant leur intégrité, leur confidentialité et leur accessibilité, y compris en cas de cessation d'activité du titulaire.

Service de validation à toute date

Le titulaire maintient, pendant toute la durée de validité des certificats émis selon les modalités prévues à sa politique de certification, un service de vérification de l'état des certificats (listes de révocation et/ou service OCSP) permettant à l'organisme bénéficiaire ou à un tiers de vérifier la validité d'un certificat à toute date dans sa période de validité.

Continuité de service et plan d'arrêt d'activité

Conformément à l'article 24 paragraphe 2 du règlement eIDAS, le titulaire dispose d'un plan d'arrêt d'activité actualisé permettant, en cas de cessation d'activité, de transférer les données d'enregistrement, les journaux et les services de révocation à un autre prestataire de service de confiance qualifié ou à un organisme désigné, dans des conditions garantissant la continuité de la valeur probante des signatures et cachets émis.

Le plan d'arrêt d'activité couvre notamment les modalités de transfert des données, les délais de mise en œuvre, l'information des organismes bénéficiaires et la continuité du service de vérification de l'état des certificats.

Gestion de la preuve en cas de litige

En tant que prestataire de service de confiance qualifié, le titulaire conserve et met à disposition de l'organisme bénéficiaire, sans surcoût, les éléments de preuve nécessaires à l'établissement de la validité d'une signature ou d'un cachet électronique, notamment l'attestation de la chaîne de certification, les éléments d'enregistrement du porteur ou du responsable du cachet, l'état du certificat à toute date durant sa période de validité et les journaux d'opérations relatifs au certificat concerné.

Le titulaire répond aux demandes de production d'éléments de preuve dans un délai de **15 jours** maximum à compter de la demande de l'organisme.

Frontière de périmètre

Le présent accord-cadre porte uniquement sur la fourniture de certificats et la mise à disposition des éléments de preuve qui s'y rapportent.

Il ne couvre pas les prestations suivantes, qui relèvent d'autres dispositifs :

- Conservation à long terme de la valeur probante des documents signés : le maintien de la validité d'une signature ou d'un cachet électronique au-delà de la durée de vie des algorithmes cryptographiques utilisés (par re-scellement ou sur-signature périodique) relève d'un service de conservation qualifié au sens du règlement eIDAS. Les organismes bénéficiaires qui ont ce besoin doivent recourir à un service distinct.
- Traçabilité de l'opération de signature : l'enregistrement de l'identité du signataire, de la date de signature et du document signé relève du parapheur ou de l'applicatif métier de chaque organisme.
- Archivage des documents signés : la conservation des documents signés relève du système d'archivage électronique de chaque organisme bénéficiaire.

4.7 Règlement général sur la protection des données (RGPD)

Le certificat de signature et le cachet électroniques doivent être en conformité avec le RGPD sur l'ensemble de ses fonctionnalités, garantir la confidentialité des documents et informations traités sur ses serveurs et ceux de ses éventuels sous-traitants. Cela concerne le traitement et stockage des données confidentielles des clients et des signataires tiers telles que le nom et prénom, l'adresse e-mail, le numéro de téléphone, l'adresse IP ou tout autre information les concernant.

5. LES PRESTATIONS ATTENDUES

5.1 Gestion du projet

Dès la notification de l'accord-cadre, le titulaire désigne un chef de projet, interlocuteur permanent et privilégié de l'UCANSS et des organismes bénéficiaires pour l'exécution de l'accord-cadre.

Lors de la réunion de lancement organisée par l'UCANSS (cf. §5.7), le titulaire présente :

- L'équipe en charge du projet ;
- Les modalités de mise à disposition ou de délivrance des certificats et des cachets, selon leur niveau ;
- Le processus pour un contrat de mandataire de certification, le cas échéant.

D'autres réunions pourront être prévues à destination des organismes afin de présenter la solution.

5.2 POC éventuels, livraison des certificats et cachets et mise en service

5.2.1 POC (Proof of concept) éventuels

Le titulaire détaillera dans son offre sa capacité à réaliser un POC à la demande d'un organisme en collaboration avec la DSI de l'organisme.

5.2.2 Commande

La commande de certificats de signature et de cachets électroniques doit se faire en ligne, via un site web ou via un portail.

5.2.3 Délivrance, livraison et accompagnement à l'usage

Le titulaire détaillera dans son offre comment se déroulera la délivrance/livraison des certificats et cachets, en fonction du type de certificat ou cachet commandé.

Le recours à un processus de mandataire de certification doit être possible.

5.3 Installation des certificats de signature et cachets électroniques sur les postes de travail et mobiles

5.3.1 Prérequis techniques

Il est attendu que le titulaire communique l'intégralité des prérequis techniques indispensables au bon fonctionnement des certificats de signature et des cachets électroniques.

5.3.2 Pilote d'installation et assistance au démarrage

Le titulaire communique, à chaque organisme commanditaire, le détail de l'installation des certificats de signature et des cachets électroniques sur les postes de travail et terminaux mobiles.

Des documents d'aide à l'installation sont transmis par le titulaire à chaque organisme commanditaire pour être ensuite mis à disposition des utilisateurs, à savoir : manuel complet d'installation et démonstration d'une signature et d'apposition d'un cachet.

Les documents doivent être rédigés en langue française et sont mis à jour à chaque modification des méthodes d'installation ou de paramétrage.

5.3.3 Délais

L'offre du titulaire indique ses délais à compter de la réception du dossier complet par type de certificat et/ou cachet.

5.4 Assistance à l'utilisation et gestion des incidents

5.4.1 Support d'assistance technique aux utilisateurs

Le titulaire doit fournir un service d'assistance aux utilisateurs des certificats de signature et des cachets électroniques.

L'offre du titulaire indique comment sont gérées les sollicitations des utilisateurs.

Le titulaire précise les horaires du support d'assistance.

L'assistance doit être disponible et joignable au moins par téléphone et par messagerie, dans les 4 heures ouvrées, du lundi au vendredi de 9H00 à 18H00 hors jours fériés.

Cette assistance technique du titulaire intervient à distance sans surcout.

Le support peut intervenir aussi bien pour des questions techniques mais aussi sur tout le cycle de vie du certificat de signature ou du cachet électronique : assistance à la commande, à l'installation, à l'utilisation, à sa révocation ou renouvellement.

Il doit être immédiatement disponible au démarrage du service et pour la durée complète du marché, et au-delà jusqu'au terme de la validité des certificats et cachets acquis.

5.4.2 Gestion des incidents remontés par les utilisateurs

Le titulaire doit s'engager de façon ferme sur sa disponibilité et sa réactivité ainsi que sur les moyens affectés à la résolution d'incidents et / ou la mise en œuvre de solutions de contournement.

Le service technique du titulaire doit pouvoir être contacté par les organismes bénéficiaires, par téléphone (hotline) ou via une plateforme Internet d'enregistrement des anomalies rencontrées.

Le support correctif de premier niveau est assuré en langue française, par une équipe de techniciens spécialisés du titulaire. L'offre du titulaire détaille les moyens humains et techniques affectés à ce support.

Le titulaire communique dès le début de la prestation, les coordonnées (numéros de téléphone, adresses mail...) et heures d'ouverture de son service de support auxquelles pourront accéder les personnes habilitées.

L'offre du titulaire décrit le processus de gestion des dysfonctionnements remontés par les utilisateurs. Il précise les modalités et les délais d'intervention. Il précise également les modalités de son suivi des anomalies déclarées par les organismes bénéficiaires, les modalités de gestion des « tickets d'incident », et ses procédures d'escalade.

5.5 Maintenance

5.5.1 Maintenance corrective

Une maintenance sera assurée par le titulaire pour corriger tout dysfonctionnement technique des certificats de signature et des cachets électroniques.

5.5.2 Évolution technique ou réglementaire

Pour toute évolution technique des certificats de signature et des cachets électroniques, l'offre du titulaire indique comment il procède pour mettre à jour les certificats de signature et les cachets électroniques existants.

En outre, pour toute évolution réglementaire, il doit s'assurer de la conformité des certificats de signatures et cachets électroniques en cours de validité et des prochains.

Le titulaire est responsable de la bonne conformité des certificats de signature et cachets électroniques utilisées.

5.6 Renouvellement et révocation

5.6.1 Renouvellement

L'offre du titulaire indique le processus de renouvellement d'un certificat de signature électronique ou d'un cachet électronique.

5.6.2 Révocation

L'offre du titulaire précise le processus de révocation pour perte du support ou pour départ de la personne physique détentrice de la signature ou disparition de la personne morale du cachet électronique.

5.7 Pilotage et Comitologie

Interlocuteurs

L'UCANSS ainsi que le Titulaire désigneront un interlocuteur permanent et privilégié dès la notification de l'accord-cadre pour son exécution.

Comité de pilotage

« Le comité de pilotage » est composé des représentants des Caisses nationales ou centrales, des représentants de l'UCANSS et du Titulaire de l'accord-cadre.

Sa mission est de définir le planning national des déploiements, ainsi que de prendre toutes autres décisions de Branche.

Une première réunion de lancement de projet a lieu lors de la notification de l'accord-cadre.

Des réunions de suivi et de pilotage des prestations sont organisées périodiquement par le comité de pilotage (généralement 1 fois par an). Elles ont pour objet l'examen :

Elles ont pour objet l'examen :

- De la bonne exécution du contrat entre les Branches et le Titulaire (suivi des déploiements, qualité de la communication, etc.) ;
- De la qualité des prestations sur les services mis en œuvre ;
- Du traitement des incidents et des actions à mener ;
- Des évolutions envisagées par chacune des parties : ajustements, changements de périmètre, évolutions réglementaires....

État du parc de certificats

Le titulaire produit et tient à jour, à destination de l'UCANSS et de chaque branche bénéficiaire, un état du parc de certificats et de cachets électroniques délivrés dans le cadre de l'accord-cadre.

Cet état du parc comporte, par organisme bénéficiaire et par branche :

- Le nombre de certificats et de cachets délivrés, ventilés par niveau eIDAS (1 à 4) et par type (signature pour personne physique, cachet pour personne morale) ;
- Le nombre de certificats et de cachets sur support cryptographique et à distance (PSE n°1 à 4) ;
- La date de délivrance de chaque certificat et cachet ;
- La date d'activation, lorsqu'elle est tracée techniquement par le titulaire ;
- La durée de validité et la date d'expiration de chaque certificat et cachet ;
- Les certificats révoqués ou suspendus en cours de validité, avec leur motif.

L'état du parc est transmis **au moins une fois par an**, en amont du comité de pilotage.

Il peut en outre être demandé à tout moment par l'UCANSS ou par une branche bénéficiaire, et est transmis dans un délai maximum de quinze jours calendaires à compter de la demande.

Au terme de l'accord-cadre, le titulaire transmet à l'UCANSS un état du parc actualisé, qui inclut notamment la liste des certificats et cachets restant en cours de validité, dans la perspective de la préparation du marché suivant.

5.8 Accompagnement et formation

Le titulaire met en œuvre les prestations suivantes, distinctes du support d'assistance technique aux utilisateurs défini au §5.4.1.

L'accompagnement à l'arbitrage et la formation préparent l'organisme aux choix et à la prise en main des certificats, tandis que le support d'assistance technique traite, au fil de l'eau, les sollicitations individuelles des utilisateurs.

Accompagnement à l'arbitrage et au recensement du besoin

À la demande d'un organisme bénéficiaire, le titulaire propose une prestation d'accompagnement à l'arbitrage et au recensement du besoin, en amont des bons de commande.

Cette prestation vise à apporter à l'organisme l'expertise du titulaire en tant que prestataire de service de confiance qualifié, afin de :

- Identifier les populations devant disposer d'un certificat de signature ou de cachet électronique au sein de l'organisme ;
- Associer chaque typologie de documents à un niveau eIDAS approprié, au regard du risque juridique et opérationnel encouru ;
- Arbitrer entre certificats sur support cryptographique et certificats à distance (PSE n°1 à 4) en fonction des cas d'usage ;
- Estimer les volumétries et le calendrier de déploiement ;
- Vérifier la compatibilité avec les parapheurs et applicatifs métier déjà utilisés par l'organisme.

La prestation se conclut par une note d'arbitrage et de recommandation remise à l'organisme bénéficiaire.

Le titulaire indique dans son offre les modalités de cette prestation (durée, profils mobilisés, livrables intermédiaires).

Formation

Le titulaire dispense, à la demande de chaque organisme bénéficiaire, des formations en français et en distanciel selon la demande de l'organisme.

La formation est dispensée à destination des profils suivants, selon les besoins de l'organisme :

Formation des mandataires de certification — elle couvre notamment :

- Le rôle et les responsabilités du mandataire de certification ;
- La procédure de vérification d'identité des porteurs ;
- La procédure de remise et d'activation des certificats et supports cryptographiques ;
- La procédure de renouvellement et de révocation ;

- La gestion des incidents et la procédure d'escalade vers le support du titulaire.

Formation des autres profils impliqués — elle peut s'adresser, à la demande de l'organisme, à d'autres profils tels que les porteurs de certificats, les responsables de cachet électronique personne morale (notamment les directeurs d'organisme), les référents en sécurité des systèmes d'information, les délégués à la protection des données, les responsables juridiques ou les équipes en charge des systèmes d'information. Le contenu de la formation est adapté au profil concerné et aux usages prévus dans l'organisme.

Une attestation de formation est délivrée par le titulaire à chaque participant formé.

Le titulaire indique dans son offre la durée, le format en distanciel, le nombre maximal de participants par session, ainsi que les supports pédagogiques remis à l'issue, pour chaque type de formation.

Guides utilisateur, administrateur et d'intégration

Le titulaire met à disposition des organismes bénéficiaires, en français et tenus à jour à chaque évolution significative du service :

- Un guide utilisateur à destination des porteurs de certificats, couvrant l'installation, l'usage courant, le dépannage de premier niveau ;
- Un guide administrateur à destination des mandataires de certification, couvrant la totalité des procédures du cycle de vie ;
- Un guide d'intégration à destination des équipes si des organismes, couvrant les prérequis techniques, la compatibilité avec les parapheurs et applicatifs métier, et les procédures de dépannage de second niveau.

Ces guides sont fournis sans surcoût et inclus dans les prestations courantes du titulaire.

Article du CCTP	Rappel des exigences auxquelles doit se soumettre le titulaire
4.2	Les certificats de signature et les cachets électroniques doivent être conformes aux normes ETSI et au Règlement eIDAS.
4.2	Le titulaire doit fournir les 4 niveaux de signature et cachet : simple niveau 1, avancée niveau 2, avec certificat qualifié niveau 3 et qualifiée niveau 4.
4.3	Le titulaire doit être qualifié eIDAS (prestataire de services de confiance qualifié – PSCQ) et s'appuyer sur une Autorité de Certification conforme eIDAS/ETSI et démontrer une maîtrise opérationnelle de la chaîne de confiance.
4.4	L'organisme peut signer tout document ou apposer son cachet pour tous les processus métiers inhérents à son fonctionnement : courriers, validation de flux financiers DCF, contrats et avenants, marchés publics, devis, ...
	Compatibilité requise avec les principaux parapheurs électroniques utilisés par les organismes. Aucune installation logicielle propriétaire requise sur les SI des organismes.
4.5	Le titulaire respecte les PSSI et les PAS-types transmis, annexés au CCTP ou communiqués en cours de marché. Il joint à sa candidature un PAS répondant aux exigences du présent CCTP.
4.6	Le titulaire respecte les exigences eIDAS et ANSSI applicables aux PSCQ.
	Il assure la traçabilité, la conservation et la mise à disposition sans surcoût des éléments de preuve. Il dispose d'un plan d'arrêt d'activité conforme à l'article 24 §2 d'eIDAS.
4.7	Le titulaire confirme sa conformité avec le RGPD. Il renseigne et joint le Questionnaire RGPD.
5.1	Dès la notification de l'accord-cadre, le titulaire désigne un chef de projet, interlocuteur permanent et privilégié de l'UCANSS et des organismes bénéficiaires. Lors de la réunion de lancement, le titulaire présente l'équipe en charge du projet, les modalités de mise à disposition ou de délivrance des certificats et des cachets selon leur niveau, ainsi que le processus pour un contrat de mandataire de certification le cas échéant.
5.2.1	Le titulaire précise sa capacité à réaliser un POC, à la demande d'un organisme, en collaboration avec sa DSI.
5.2.2	La commande de certificats de signature et de cachets électroniques se fait en ligne via un portail mis à disposition par le titulaire. Le portail est sécurisé par authentification forte des utilisateurs, journalisation horodatée des opérations, et fait l'objet d'audits PASSI périodiques. Les incidents de sécurité affectant le portail sont notifiés au pouvoir adjudicateur (RGPD, bonnes pratiques ANSSI).

5.2.3	Le titulaire doit décrire les modalités de mise à disposition d'un certificat de signature simple (Niveau 1 eIDAS).
	Le titulaire doit décrire les modalités de mise à disposition d'un certificat de signature avancée (Niveau 2 eIDAS)
	Le titulaire décrit les modalités de délivrance d'un certificat de signature électronique avancée fondée sur un certificat qualifié (Niveau 3 eIDAS) par un prestataire de services de confiance qualifié, dans le respect de l'article 26 du Règlement eIDAS.
	Le titulaire décrit les modalités de délivrance d'un certificat de signature électronique qualifiée (Niveau 4 eIDAS). Il est rappelé que certains organismes sont en outre-mer.
	Le titulaire doit décrire les modalités de délivrance d'un certificat de type cachet électronique pour personne morale, en fonction du niveau (1 à 4).
	Le recours à un processus de mandataire de certification doit être possible. Le processus sera décrit.
5.3.1	Le titulaire communique l'intégralité des prérequis techniques indispensables au bon fonctionnement des certificats de signature et des cachets électroniques.
5.3.2	Le titulaire communique le détail de l'installation des certificats sur les postes de travail et terminaux mobiles, et précise la disponibilité de la documentation associée.
5.3.3	Le titulaire indiquera ses délais de délivrance de chaque certificat de signature et cachet électroniques.
5.4.1	Support : le titulaire indique comment sont gérées les sollicitations des utilisateurs. Le titulaire précise les horaires du support d'assistance. Il confirme sa disponibilité jusqu'au terme de la validité des certificats ou cachets acquis.
5.4.2	Gestion des incidents : Le titulaire décrit le processus de gestion des dysfonctionnements remontés par les utilisateurs. Il précise les modalités et les délais d'intervention. Il précise également les modalités de son suivi des anomalies déclarées par les organismes bénéficiaires, les modalités de gestion des « tickets d'incident », et ses procédures d'escalade.
5.5.1	Maintenance corrective : le titulaire corrige tout dysfonctionnement technique des certificats de signature et des cachets électroniques.
5.5.2	Le titulaire précise comment il prend en compte les évolutions techniques ou réglementaires.
5.6.1	Le titulaire indique le processus de renouvellement d'un certificat de signature électronique ou d'un cachet électronique.
5.6.2	Le titulaire précise le processus de révocation pour perte du support ou pour départ de la personne physique détentricice de la signature ou disparition de la personne morale du cachet électronique.

5.7	L'UCANSS et le titulaire désignent chacun un interlocuteur permanent et privilégié. Un comité de pilotage annuel est organisé entre l'UCANSS, les caisses nationales et centrales et le titulaire. Le titulaire produit et tient à jour un état du parc des certificats et cachets délivrés (par organisme, par branche, par niveau eIDAS, avec dates de délivrance, d'activation et d'expiration), transmis au moins une fois par an et à tout moment sur demande dans un délai de 15 jours.
5.8	Le titulaire propose, en complément du support défini au §5.4.1 : (i) un accompagnement à l'arbitrage et au recensement du besoin pour le choix des certificats par typologie de documents et niveau de risque ; (ii) des formations destinées aux mandataires de certification et aux autres profils impliqués (porteurs, responsables de cachet personne morale, DPO, juristes, équipes SI), en français et en distanciel, avec attestation ; (iii) des guides utilisateur, administrateur et d'intégration en français, tenus à jour ; (iv) une prestation d'accompagnement à la conduite du changement.

Est annexé à l'acte d'engagement, le cadre de réponse technique. A ce titre, le cadre de réponse est contractuel.