



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Secrétariat général

DIRECTION DE LA TRANSFORMATION NUMERIQUE (DTNUM)

**SOUS-DIRECTION DES APPLICATIONS NUMERIQUES
(SDAN)**

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(CCTP)**

**ACCORD-CADRE RELATIF A LA
CONCEPTION, LE DEVELOPPEMENT, LA MAINTENANCE DU
COMPOSANT BIOMÉTRIQUE DU MINISTERE DE L'INTERIEUR
« CBIMI »**

Le présent CCTP comporte les annexes suivantes :

Annexe 1	Découpage des prestations et des livrables (DPL)
Annexe 2	PAS Modèle
Annexe 3	PAQ Modèle
Annexe 4	CCT du Ministère de l'Intérieur
Annexe 5	Story Mapping MVP du composant de captation

SOMMAIRE

I.	PRESENTATION DE L'ACCORD CADRE	7
I.1	Contexte et Objet de l'accord cadre.....	7
I.2	Enjeux	8
I.3	Présentation de la maîtrise d'ouvrage et de la maîtrise d'œuvre.....	9
I.4	Structure de l'accord cadre	10
II.	PRESENTATION DU CBIMI	11
II.1	Présentation générale	11
II.2	Description des fonctionnalités des différents composants	12
II.3	Composant de Captation	12
II.4	Composant Noyau Biométrie	14
II.5	Composant d'Adjudication	15
II.6	Interfaces d'échange.....	16
II.7	Module d'observabilité	17
II.8	Principe d'instanciation	18
II.9	Calendrier prévisionnel	18
III.	GOVERNANCE DE L'ACCORD CADRE	19
III.1	Le comité de pilotage (COPIL).....	19
III.2	Le comité de Suivi MOE (COSUI MOE)	20
III.3	Le comité technique (COTECH)	21
III.4	Le comité de sécurité (COSEC).....	22
III.5	Le comité Contractuel(COCON)	22
IV.	SOCLE TECHNIQUE	23
IV.1	Principes généraux	23
IV.2	Stratégie d'APIsation.....	23
IV.3	Supervision et monitoring de la solution cible.....	23
IV.4	Principes de sécurisation	23
IV.5	Technologies utilisées et socle de développement du titulaire.....	24
IV.6	Chaîne industrielle du Ministère.....	24
IV.7	Développements chez le titulaire	24
IV.8	Piles logicielles.....	25
V.	EXIGENCES COMMUNES À L'ENSEMBLE DES PRESTATIONS	27
V.1	Exigences générales.....	27
V.2	Exigences sur la documentation	27
V.3	Exigences sur la conduite des prestations.....	30
V.4	Exigences sur la gouvernance.....	31
V.5	Exigences sur les ressources du titulaire.....	32
V.6	Exigences sur les moyens techniques et sur la cohérence de l'architecture technique globale du système d'information	34

V.7	Exigences sur les vérifications et contrôle qualité	35
V.8	Exigences SSI	35
V.9	Exigences sur la résolution des anomalies.....	36
VI.	DISPOSITIONS COMMUNES A L'ENSEMBLE DES PRESTATIONS.....	38
VI.1	Lieux d'exécution et télétravail	38
VI.2	Dossier de pilotage, tableaux de bord et indicateurs	38
VI.3	Horaires d'exécution	38
VII.	LOT 1 : CONCEPTION, DEVELOPPEMENT ET MAINTENANCE DES BRIQUES LOGICIELLES DU CBIMI.....	39
VII.1	Présentation du Lot 1	39
VII.2	Équipe du titulaire	39
VII.3	Présentation de la démarche agile pour le Lot 1	40
VII.4	L'équipe multidisciplinaire et la vision produit	40
VII.5	L'agilité à grande échelle	41
VII.6	L'agilité à petite et moyenne échelle	42
VII.7	L'excellence technique.....	43
VII.8	Une approche UX en continu	43
VII.9	Optimisation du Time to Citizen et du Time to Repair	43
VII.10	Démarche de tests, d'intégration et de déploiement en continu.....	43
VII.11	Définition de terminé ou « Definition of Done » ou « DoD »	44
VII.12	Gouvernance de la démarche agile et disponibilité des intervenants	44
VII.13	Rituels équipe	44
VII.14	Disponibilité des intervenants et stabilité de l'équipe	45
VII.15	Vélocité.....	45
VII.16	Méthode d'estimation de l'effort.....	46
VII.17	Engagements liés au bon fonctionnement.....	46
VII.18	Mesure de la performance (Métriques).....	46
VII.19	Taux d'échec des changements :	47
VII.20	Prestation L1P1 - Initialisation de l'accord cadre, prise de connaissance du CBIMI et Reprise du composant de captation	48
VII.21	Prestation L1P2 - Étude de faisabilité	50
VII.22	Prestation L1P3 - Réalisation et maintenance du CBIMI en mode Agile	51
VII.23	Prestation L1P4 – Réversibilité	58
VIII.	LOT 2 : FOURNITURE DES MIDDLEWARE MAINTENANCES ASSOCIEES ET EXPERTISES61	
VIII.1	Présentation du Lot 2	61
VIII.2	Définition	61
VIII.3	Normes applicables sur les composants biométriques.....	63
VIII.4	Environnements de fonctionnement	64
VIII.5	Gestion des licences	65
VIII.6	Équipe du titulaire	66

VIII.7	Prestation L2P1 - Fourniture de Middleware et maintenances associées.....	66
VIII.8	Prestation L2P2 – Fourniture de dongles garantie standard incluse	69
VIII.9	L2P3 – Assistance, expertises et formations	70
VIII.10	Prestation L2P4 - Conception et développement de nouvelles fonctionnalités Middleware (hors roadmap éditeur).....	72
VIII.11	Prestation L2P5 - Réversibilité	73
VIII.12	Prestation L2P6 Transfert des licences Middleware sur un autre mode d'hébergement	74
IX.	LOT 3 : FOURNITURE DES COMPOSANTS DU « NOYAU BIOMETRIQUE », ADJUDICATION, FOURNITURE DE SOLUTION DE CHIFFREMENT, MAINTENANCES ASSOCIEES ET EXPERTISES	76
IX.1	Présentation du Lot 3	76
IX.2	Gestion des licences pour les AFIS/ ABIS et le logiciel d'adjudication.....	76
IX.3	Équipe du titulaire	78
IX.4	Prestation L3P1 - Fourniture d'AFIS ou d'ABIS pour le composant « noyau biométrie » et maintenances associées.....	78
IX.5	Prestation L3P2 Transfert des licences AFIS/ABIS sur un autre mode d'hébergement	81
IX.6	Prestation L3P3 - Fourniture du logiciel d'adjudication et maintenances associées	82
IX.7	Prestation L3P4 Transfert des licences du logiciel d'adjudication sur un autre mode d'hébergement	85
IX.8	Prestation L3P5 - Fourniture de solutions de chiffrement et maintenances associées	86
IX.9	Prestation L3P6 – Assistance, expertises et formations pour l'ensemble des produits biométriques du lot 3.....	91
IX.10	Prestation L3P7 - Conception et développement de nouvelles fonctionnalités biométriques (hors roadmap éditeur) pour l'ensemble des produits biométriques du lot 3.....	92
IX.11	Prestation L3P8 – Fourniture de dongles garantie standard incluse	93
IX.12	Prestation L3P9 - Réversibilité.....	94

TERMES ET ABRÉVIATIONS

Abréviations

AMOA	Assistance à Maîtrise d'Ouvrage
AMOE	Assistance à Maîtrise d'Œuvre
APM	« <i>Application Performance Management</i> » Gestion de la performance des applications
API	Interface de programmation d'application
BADM	Bureau des applications des directions métiers
BFO	Bureau de la fiabilisation des opérations
CBIMI	Composants Biométriques du Ministère de l'intérieur
CCAP	Cahier des clauses administratives particulières
CCTP	Cahier des clauses techniques particulières
CCT	Cadre de Cohérence Technique
CI / CD	Intégration continue / Déploiement continu
CNIL	Commission Nationale de l'Informatique et des Libertés
DC	Déploiement contenu
DCE	Dossier de consultation des entreprises
DTNUM	Direction de la Transformation Numérique du Ministère de l'Intérieur
MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
MI	Ministère de l'intérieur
MOA	Maître d'ouvrage
MOE	Maître d'œuvre
PAQ	Plan d'assurance qualité
PAS	Plan d'assurance sécurité
PI	Program increment
PO	Product Owner
PPO	Proxy Product Owner
PV	Procès-verbal

SOA	« <i>Service Oriented architecture</i> » Architecture orientée service
SSI	Sécurité des Systèmes d'Information
TMA	Tierce Maintenance Applicative
VM	Machine virtuelle
DGEF	Direction générale des étrangers en France
MINUM	Mission du Numérique – DGEF

Termes employés

Backlog	Ensemble des besoins recueillis et priorisés par le PO pour créer le produit cible désiré.
Cloud PI	Cloud privé du ministère de l'intérieur : Produit du ministère de l'intérieur
DevOps	Ensemble de pratiques et d'outils, qui permettent d'automatiser et d'intégrer les processus entre les équipes de développement et des opérations informatiques.
Epic	Est définit comme un niveau supérieur à la « <i>feature</i> ».
Feature	(Fonction) est un ensemble de « <i>User Stories</i> » (US)
Incrément	Constitue un ensemble d'itération (généralement 5)
ISOCELE	Environnement VMWare de la DTNUM
Itération	Synonyme Sprint Désigne une séquence courte pendant laquelle l'équipe va travailler sur l'accomplissement d'un objectif. (généralement 2 semaines/ 10 jours ouvrés)
Poker Planning	Mode d'estimation de l'effort de développement d'une fonctionnalité selon la méthode Agile SCRUM.
Release	Une <i>release</i> est une nouvelle version du produit, livrée aux utilisateurs et destinée à être mise en production. Elle est le résultat de plusieurs itérations.
User story (US)	Une user story est une phrase simple, exprimée dans un langage commun et permettant de décrire avec suffisamment de précision le contenu d'une fonctionnalité à développer. La phrase contient généralement trois éléments descriptifs de la fonctionnalité : Qui ? Quoi ? Pourquoi ? Elle peut être formalisée comme suit : « En tant que <qui>, je veux <quoi> afin de <pourquoi> ». Une user story traduit le point de vue métier Elle contient les critères d'acceptance qui décrivent les conditions de validations de l'US.
Middleware	Un middleware est un gestionnaire de matériels qui permet de piloter des périphériques (capteurs d'empreintes, lecteur/scanner de documents, caméra/ prise d'images faciales...).

PSE	<p>Les prestations supplémentaires éventuelles (PSE) concernent les prestations éventuellement proposées dans l'offre du titulaire à la demande de l'administration.</p> <p>Les PSE qui peuvent être présentées par les candidats sont limitativement identifiées dans le CCAP et dans les AF. Les PSE ne sont pas prises en compte dans l'analyse des offres.</p> <p>Dès lors, l'absence de présentation de PSE ne rend pas l'offre irrégulière.</p>
------------	---

I. PRESENTATION DE L'ACCORD CADRE

I.1 CONTEXTE ET OBJET DE L'ACCORD CADRE

Le ministère de l'intérieur utilise la biométrie dans le cadre de l'exercice de plusieurs missions principales, telles que la délivrance des titres officiels, le contrôle aux frontières, le contrôle de l'immigration, de l'asile et de la situation des ressortissants étrangers, la sécurité publique et les enquêtes judiciaires, etc. Cet usage se fait dans un cadre réglementaire strict et protecteur des libertés et des données personnelles. Les données biométriques servant à identifier les personnes de manière sûre et fiable peuvent être de plusieurs natures, les principales étant les empreintes digitales et la photo de face. D'autres données peuvent être utilisées pour des finalités précises conformément à la loi, telles que les empreintes palmaires et les empreintes génétiques.

Plusieurs applications biométriques sont aujourd'hui utilisées par le Ministère de l'Intérieur pour acquérir, enregistrer et consulter ces données. Quelle que soit la finalité métier, ces applications répondent à une architecture globalement commune, une couche métier spécifique portant la synoptique métier et des fonctions biométriques enrôlement, authentification, identification, adjudication.

Ces applications, bien que performantes, présentent une gestion complexe, notamment en ce qui concerne leur évolution, leur maintenance et leur interopérabilité :

- Les fonctions biométriques sont dupliquées et hétérogènes, ce qui ne permet pas de réelle capitalisation et oblige à dupliquer les adaptations comme la prise en compte d'un nouveau type de capteur ;
- La non séparation des fonctions métier des fonctions biométriques a conduit à la création d'applications spécifiques rendant difficile voire impossible la montée de version des produits et ainsi bénéficier des nouveautés, comme le remplacement des clients lourds par des clients légers. Elle oblige aussi à confier le développement de fonctions métier à un éditeur de solution biométriques dont ce n'est pas le cœur de métier ;
- Le manque d'outil d'observabilité complexifie notamment l'analyse des problèmes liés aux périphériques : capteurs, lecteurs de titre.

L'arrivée à échéance de plusieurs marchés biométrie, des initiatives récentes autour de la biométrie comme NéoDK ou Bioweb ainsi que la généralisation de l'utilisation de la biométrie au niveau des nouveaux systèmes d'information Européens ont conduit la Sous-Direction des Applications Numériques (SDAN) de la DTNUM à commander une étude sur l'harmonisation, la rationalisation des applications biométriques conduisant aux recommandations suivantes :

- Urbanisation des applications biométriques, en adoptant une architecture modulaire, flexible, évolutive et sécurisée en séparant les fonctions métiers des fonctions biométriques et en mutualisant ces dernières ;
- Regroupement des fonctions biométriques mutualisées en une offre de service ministérielle portée par une équipe dédiée et adressant toute nouvelle application biométrique.

Cette offre de service ainsi ciblée est identifiée sous l'intitulé CBIMI (ci-après Composants Biométriques du Ministère de l'Intérieur). Cette offre devra répondre aux besoins de modernisation des outils existants tout en garantissant la sécurité, l'efficacité et la conformité des solutions mises en place.

L'objet du présent marché est de concevoir, développer / construire et maintenir cette offre de service (CBIMI) en y intégrant l'ensemble des fonctions biométriques nécessaires aux applications biométriques, tout en offrant une parfaite interopérabilité avec les équipements biométriques (capteurs, ...) dans une infrastructure parfaitement sécurisée.

Ce présent marché s'inscrit dans le cadre du plan de modernisation et de transformation numérique portée par la direction de la transformation numérique. Il répond également aux nécessités d'évolutions croissantes des systèmes européens (ex : EUODAC « PFSE III », VIS, EES) en matière de biométrie et aux initiatives en matière d'amélioration des systèmes déjà engagées à l'échelle nationale et européenne (ex : Visabio, Bioweb, CCAF, NeoDK... ;.).

I.2 ENJEUX

Dans un contexte où l'intelligence artificielle générative permet de produire des contenus trompeurs permettant difficilement de discerner les contenus authentiques des faux et compte tenu du rôle croissant de la biométrie dans les dispositifs visant à améliorer la sécurité et la lutte contre la fraude grâce à l'identification ou l'authentification d'un individu à partir de ses caractéristiques physiques ou comportementales uniques ; la SDAN a souhaité mettre au centre la stratégie biométrie applicative afin d'en renforcer la maîtrise par le ministère de l'intérieur, d'anticiper les changements et les innovations à venir.

Pour porter cette stratégie, un pôle d'expertise biométrique applicative organisé autour **3 axes** a été créé en 2024 :

- **un axe opérationnel** qui a en charge l'offre CBIMI : sa construction, sa mise en œuvre, son maintien, son évolution et son intégration dans les applications biométriques avec leur support ;
- **un axe prospectif** qui permet d'être toujours à l'état de l'art et de suivre les tendances et les recherches dans ce domaine tout en gardant le regard opérationnel ;
- **un axe communautaire** qui permet au niveau du MI, le partage des connaissances en la matière et la mutualisation des besoins et des forces.

L'offre de services visée au travers des Composants Biométriques du Ministère de l'Intérieur (CBIMI) a pour but de favoriser la maîtrise des solutions biométriques par le MI, et de faciliter leur évolution et maintien en conditions opérationnelles dans le cadre d'un socle de composants unifiés.

En outre, cette offre se veut évolutive et adaptable aux besoins futurs avec des solutions standard, optimisées et à l'État de l'Art, elle vise également à améliorer la qualité de service rendu aux utilisateurs grâce notamment à l'intégration native de fonctions d'observabilité

Dans le cadre de la démarche de modularité voulue par l'administration, les logiciels standards biométriques pourront être implémentés indépendamment les uns des autres, appelés et déployés de manière unitaire ou bien décommissionnés en fin de marché.

Les enjeux identifiés sont globalement les suivants :

- **Rationaliser** les fonctions biométriques ;
- **Maîtriser** le présent et la trajectoire des futures implémentations ;
- **Optimiser** les ressources financières ;
- **Simplifier** les procédures existantes ;
- **Réduire** le time to market des nouvelles applications biométriques ;
- **Fiabiliser** les services, permettre la pro-activité et améliorer la qualité de service auprès de nos utilisateurs.

Le CBIMI doit notamment être capable :

- De permettre à toutes les applications d'utiliser les mêmes périphériques (le même capteur digital, lecteur de document, scanner, prise d'images faciales, etc...), et limiter les évolutions nécessaires à l'intégration des périphériques utilisés dans les applications.
- De s'adapter à de nouveaux périphériques sans impacter les applications métiers.
- De garantir que les logiciels standards biométriques soient implémentés de manière indépendante, appelés et déployés de façon unitaire, ou décommissionnés à la fin du contrat, conformément à la démarche de modularité souhaitée par le ministère. Le composant logiciel propriétaire (éditeurs) et les développements spécifiques devront cohabiter sans dépendance mutuelle.

Les systèmes de bases de données européens (tels que les SI EURODAC/PFSE III, VIS) étant en évolution constante, l'exigence en matière d'interopérabilité et de maintenance évolutives est une exigence de premier ordre. Le nouveau système (CBIMI) doit donc permettre le développement d'applications biométriques plus simples et plus rapides sans incompatibilité entre elles ou avec les capteurs.

Il faut noter que les données biométriques sont des données personnelles sensibles dont le traitement est encadré par le RGPD.

I.3 PRESENTATION DE LA MAITRISE D'OUVRAGE ET DE LA MAITRISE D'ŒUVRE

Le présent accord cadre est porté par la Sous-Direction des Applications Numériques (ci-après SDAN) de la Direction de la Transformation Numérique du Ministère de l'Intérieur (DTNUM).

La sous-direction des applications numériques conçoit et réalise les applications du ministère au profit des directions « métier » du ministère de l'intérieur. Elle garantit la qualité des services en production, à ce titre elle assure la maintenance de son patrimoine applicatif au niveau de performance requis. Elle met en œuvre les démarches agiles. Cette dernière vise à délivrer rapidement et avec le moins de dérive possible, des produits sécurisés et de qualité centrés sur les besoins utilisateurs.

Le pôle biométrie de la section Produit Migratoire et Biométrie Applicative (PMeBA) du Bureau des Applications des Directions Métiers (BADM) de la Sous-Direction des Applications Numériques (SDAN) intervient en tant que maître d'ouvrage et maître d'œuvre sur le CBIMI et pilote à cet effet le présent accord-cadre sur le plan opérationnel et contractuel.

La maîtrise d'ouvrage est partagée entre pôle biométrie et la MINUM et les directions métiers (ou directions d'application) de la DGEF représentante des différentes directions métiers, nous nommerons cet ensemble MOA dans la suite du document.

I.4 STRUCTURE DE L'ACCORD CADRE

Le présent accord-cadre se compose de **trois lots** comme suit :

LOT 1	Conception, développement et maintenance des briques logicielles du CBIMI
Prestation L1P1	Initialisation de l'accord cadre et prise de connaissance du CBIMI et reprise du composant de captation
Prestation L1P2	Étude de faisabilité
Prestation L1P3	Réalisation et maintenance du CBIMI en mode Agile
Prestation L1P4	Réversibilité

LOT 2	Fourniture des middleware, maintenances associées et expertises
Prestation L2P1	Fourniture de middleware et maintenances associées
Prestation L2P2	Fourniture de Dongles garantie standard incluse
Prestation L2P3	Assistance, expertises et formations
Prestation L2P4	Conception et développement de nouvelles fonctionnalités Middleware (hors roadmap éditeur)
Prestation L2P5	Réversibilité
Prestation L2P6	Transfert des licences Middleware sur un autre mode d'hébergement

LOT 3	Fourniture des composants « noyau biométrie », adjudication, fourniture de solutions de chiffrement, maintenances associées et expertises
Prestation L3P1	Fourniture d'AFIS ou d'ABIS pour le composant « noyau biométrie » et maintenances associées
Prestation L3P2	Transfert des licences AFIS/ABIS sur un autre mode d'hébergement
Prestation L3P3	Fourniture du logiciel d'adjudication et maintenances associées
Prestation L3P4	Transfert des licences du logiciel d'adjudication sur un autre mode d'hébergement
Prestation L3P5	Solutions de chiffrement
Prestation L3P6	Assistance, expertises et formations pour l'ensemble des produits biométriques du lot 3
Prestation L3P7	Conception et développement de nouvelles fonctionnalités biométriques (hors roadmap éditeur) pour l'ensemble des produits biométriques du lot 3
Prestation L3P8	Fourniture de dongles garantie standard incluse
Prestation L3P9	Réversibilité

II. PRESENTATION DU CBIMI

II.1 PRESENTATION GENERALE

Les composants biométriques du ministère de l'intérieur (CBIMI) constituent des « briques » modulaires conçues pour accélérer le développement de nouvelles applications biométriques. En tant que composants mutualisés, ils peuvent être réutilisés dans différents contextes. Chaque application biométrique métier intégrera une ou plusieurs instances de ces composants, en fonction de ses besoins spécifiques. Par exemple, une application biométrique peut ne pas nécessiter le composant d'adjudication, selon le scénario d'utilisation.

Le schéma suivant illustre les composants du CBIMI sur laquelle l'offre de service s'appuie :

Architecture d'un application biométrique avec CBIMI

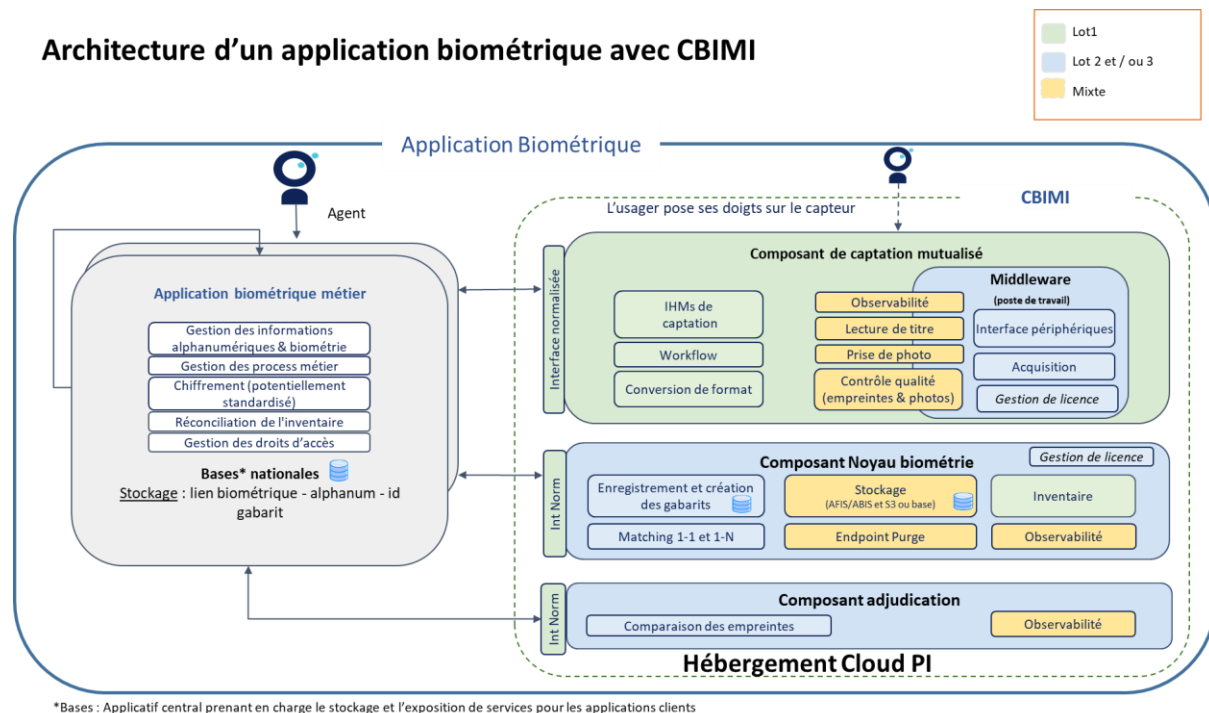


Figure 1 : Offre de service CBIMI

Le composant de captation:

Le composant de captation gère l'acquisition des données biométriques entre autres à partir de périphériques tels que des capteurs d'empreintes, lecteurs de cartes biométriques, matériel de prise d'image faciale ou capteurs d'iris. Ce composant est la propriété de l'administration.

Pour fonctionner, ce composant applicatif nécessite une couche intermédiaire que l'on appelle : middleware (produit éditeur).

Ces middlewares sont des gestionnaires de matériels qui permettent de piloter des périphériques (capteurs d'empreintes, lecteur/scanner de documents, caméra/ prise d'images faciales...). Ils prétraitent et valident les données avant transmission au système de gestion biométrique. Ils assurent également la communication entre ces périphériques et le système, normalisant les données capturées et garantissant leur transmission sécurisée vers le système de gestion biométrique.

Le composant Noyau : Génération, stockage et comparaison des gabarits :

Le composant noyau transforme les données biométriques brutes en gabarits (représentations mathématiques compactes). Il génère, stocke et compare ces gabarits (empreintes, images faciales,

etc.) pour effectuer des opérations d'identification ou d'authentification via les algorithmes de détection de similarité, permettant de valider l'identité d'un individu en fonction du score de comparaison.

Le composant d'adjudication :

L'adjudication permet à un utilisateur de statuer sur deux données biométriques présentant un seuil de similitude identifié par les algorithmes de comparaison. Elle permet de statuer sur la validité d'une correspondance en fonction du score de similarité entre deux gabarits biométriques.

Les solutions de chiffrement :

Les solutions de chiffrement assurent la sécurité des échanges entre la base de données métiers alphanumériques et la base de données biométriques. **Elles peuvent être virtualisées ou sous forme de matériels.**

Elles utilisent des protocoles pour garantir la confidentialité et l'intégrité des données sensibles transmises, conformément aux normes de sécurité et de protection des données.

Au titre de la démarche de modularité voulue par l'administration, chaque composant doit pouvoir être implémenté indépendamment des autres, appelé et déployé de manière unitaire ou bien décommissionné en fin de marché pour être remplacé sans impacter les autres composants

L'ensemble des licences acquises au titre des produits précités (hors composant de captation) faisant l'objet d'une tarification au titre de l'annexe I à l'acte d'engagement « annexe financière » doivent pouvoir être déployé sur l'ensemble des environnements (production et hors production).

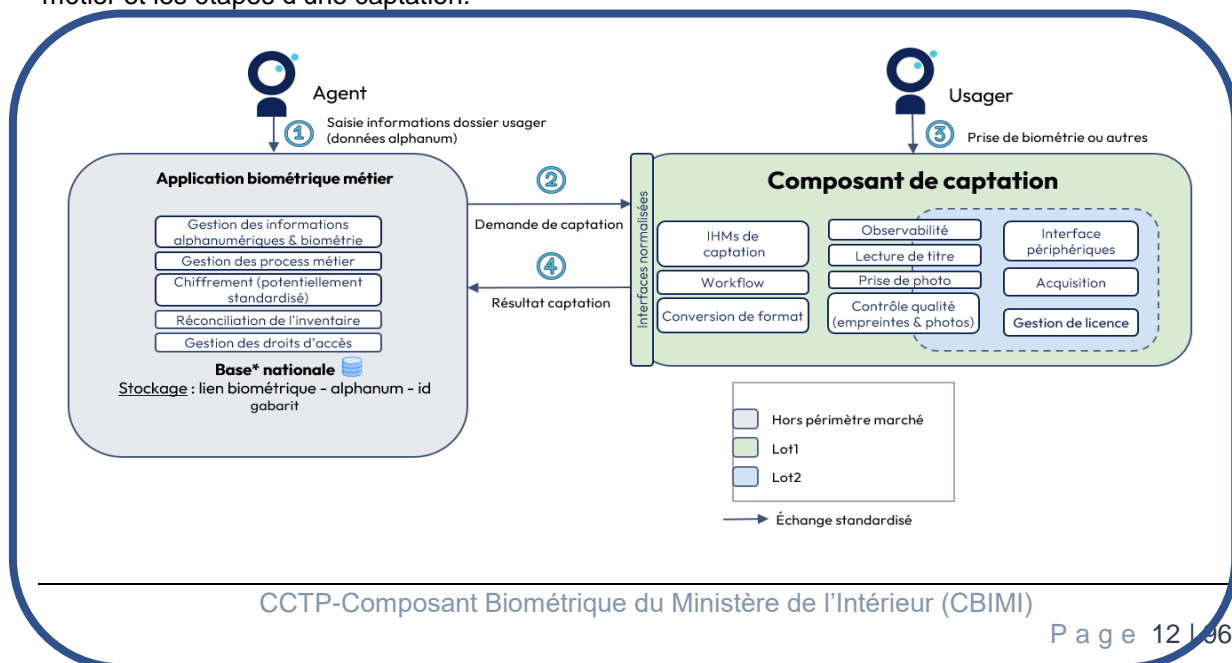
II.2 DESCRIPTION DES FONCTIONNALITES DES DIFFERENTS COMPOSANTS

II.3 COMPOSANT DE CAPTATION

L'objectif de ce composant est de faciliter la captation de divers types de données (biométriques ou non) à partir de différents périphériques tels que des capteurs d'empreintes digitales, des matériels de prise d'image, des scanners, des lecteurs de titres, ou encore via le téléchargement de documents et autres dispositifs. Il permet d'effectuer des contrôles qualité, de vérifier le respect des normes, de rejouer la captation ou de limiter son périmètre. Ce composant ne traite pas les données métiers, ce qui lui permet d'être facilement intégré dans des applications biométriques, contribuant ainsi à réduire leur temps de développement. Il est conçu pour être mutualisé et réutilisé pour plusieurs applications biométriques (une instance pour une application métier).

Ce composant étant activé par une application métier biométrique, la nature de la demande, le type et le niveau des contrôles, le format attendu lui sont communiqués par cette application via un contrat d'échange normalisé.

Le schéma ci-dessous illustre le composant de captation et son lien avec une application biométrique métier et les étapes d'une captation.



Application Biométrie

Figure 2: Illustration de l'usage du composant de captation

Le retour d'expérience de l'utilisation des applications biométriques existantes montre un besoin de contrôle de l'état du capteur et de sa liaison, ainsi que la connaissance des actions effectuées par l'agent. Le composant de captation trace en base de données toutes ces informations pouvant être utilisées en monitoring ou en observabilité. Une interface utilisateur (IHM) est à développer afin qu'un administrateur puisse disposer facilement de ces informations.

Un produit minimum viable (PMV) existe, il est composé d'écrans :

- Listant les capteurs connectés au poste de l'utilisateur et leurs états ;
- Guidant l'agent en charge de l'acquisition des empreintes dans les étapes de la captation
- Affichant les niveaux de qualité,
- Offrant la possibilité d'indiquer des exceptions, d'abandonner, de faire un retour en arrière, ou de la valider après avoir visualisé le récapitulatif.

Le workflow ou enchaînement des écrans du composant de captation est en partie piloté par l'interface d'échange avec l'application biométrique métier.

La conversion de format peut générer des fichiers NIST de différentes versions (2011, 2015, etc.), ainsi que des fichiers dans d'autres formats tels que WSQ, JPEG, etc.

Comme indiqué précédemment, il est conçu pour fonctionner avec différents types de périphériques, et pourra évoluer pour en intégrer d'autres à l'avenir.

Le composant de captation s'appuie sur les middleware fournis par le titulaire du lot 2, installés sur les postes utilisateurs et qui communiquent avec les périphériques, lui permettant ainsi de recueillir les informations et données nécessaires pour répondre à la demande, mesurer la qualité et connaître l'état du capteur notamment.

Le tableau suivant présente la liste des fonctionnalités minimales du composant de captation :

FONCTIONNALITES	FONCTION	DESCRIPTION
IHM de captation	Interface utilisée pour interagir avec le capteur	L'IHM (Interface Homme-Machine) permet à l'utilisateur de voir et contrôler le processus de capture biométrique.
Workflow	Ensemble des étapes de traitement des données capturées	Le workflow définit le chemin que suivent les données après leur capture, depuis l'enregistrement jusqu'à l'analyse.
Conversion de format	Transformation des données biométriques dans un format standard	Les données capturées sont souvent converties (ex. JPEG, NIST...) pour être compatibles avec d'autres systèmes.
Observabilité	Surveillance et contrôle de l'état du capteur, de toute action utilisateur et des processus associés	Cela permet de détecter les problèmes (pannes, erreurs) et de s'assurer que le capteur fonctionne correctement.
Lecture de titre	Extraction des informations textuelles d'un document	Cette fonction complète la capture biométrique en lisant les données écrites (ex. passeport, carte d'identité).

Contrôle de qualité empreinte et photos	Vérification de la clarté et de la précision des données capturées	Le système évalue si les empreintes ou les photos sont suffisamment nettes pour être utilisées efficacement.
Interfaces périphériques	Connexion à d'autres appareils ou systèmes	Le capteur communique avec des systèmes externes (ex. bases de données, imprimantes) via des interfaces standard.
Acquisition	Processus de capture des données biométriques	C'est l'étape initiale où le capteur collecte les empreintes, visages ou iris de l'utilisateur par exemple.

II.4 COMPOSANT NOYAU BIOMETRIE

Le composant noyau biométrique a trois fonctions principales :

- L'enrôlement biométrique consistant à enregistrer les données biométriques en base de données. Plus précisément il y a la création du gabarit et son enregistrement en base. Le gabarit ainsi enregistré sert lors de la phase d'identification et d'authentification. À des fins de preuves mais aussi d'évolutivité et de réversibilité des systèmes biométriques.;
- L'identification et l'authentification qui sont assurées par le comparateur aussi nommé « matcheur ». Le comparateur s'appuie sur les gabarits présents sur une carte à puce ou en base centrale pour calculer une distance ou score de similarité.
 - o L'authentification qui calcule une similarité entre un gabarit extrait d'une capture et un gabarit extrait d'une image brute sur support biométrique (passeport, titre de voyage, visa, ...) (aussi nommée recherche 1:1) ; Cette étape peut être précédée par une recherche alphanumérique.
 - o L'identification qui calcule une similarité entre un gabarit d'une capture et tous les gabarits présents en base centrale (communément appelée recherche 1: N).
- Le composant Noyau n'a pas vocation à travailler sur des données métiers comme le nom, prénom ...

Le tableau suivant présente la liste des fonctionnalités minimales du composant noyau en partie fondée sur les fonctionnalités des AFIS ou ABIS :

FONCTIONNALITES	FONCTION	DESCRIPTION
Création et enregistrement des gabarits en base	Création de modèles biométriques à partir des données capturées	Le composant noyau transforme les données brutes en gabarits biométriques uniques utilisés pour l'identification et l'authentification.
Stockage en base et / ou sur une autre support des gabarits avec un identifiant technique (ID gabarit, gabarit).	Enregistrement sécurisé des gabarits biométriques avec un identifiant unique	Chaque gabarit est stocké sous forme de clé (ID unique) et valeur (données biométriques) pour faciliter la recherche et la récupération.
Inventaire	Liste des identifiants des gabarits et de leur état présent en base de données	Le système maintient un inventaire de tous les gabarits enregistrés permettant de garantir la synchronisation des bases

		noyau et application biométrique métier
Matching 1 :1 et 1 : N	Fonction d'interrogation des gabarits de la base à partir de données biométriques capturées Comparaison des gabarits pour l'identification et l'authentification	Le Matching 1 :1 compare un gabarit avec un gabarit cible précis, tandis que le 1 :N compare un gabarit à plusieurs pour trouver une correspondance.
Endpoint Purge	Traitement de suppression sécurisée des gabarits à partir d'une liste d'identifiants mais également suppression	Cette fonction garantit que les données biométriques sont supprimées de la base de données de manière sécurisée en produisant un rapport de purge
Observabilité	Surveillance continue des performances et de l'état du système	Le système suit les performances, les erreurs et l'état global du composant central pour assurer une disponibilité et une fiabilité maximales.

II.5 COMPOSANT D'ADJUDICATION

Lorsque lors de la création des gabarits deux biométries sont similaires, le composant d'adjudication dispose d'outils permettant à un agent de comparer visuellement les biométries afin de déterminer si elles sont identiques.

Zoom sur l'adjudication

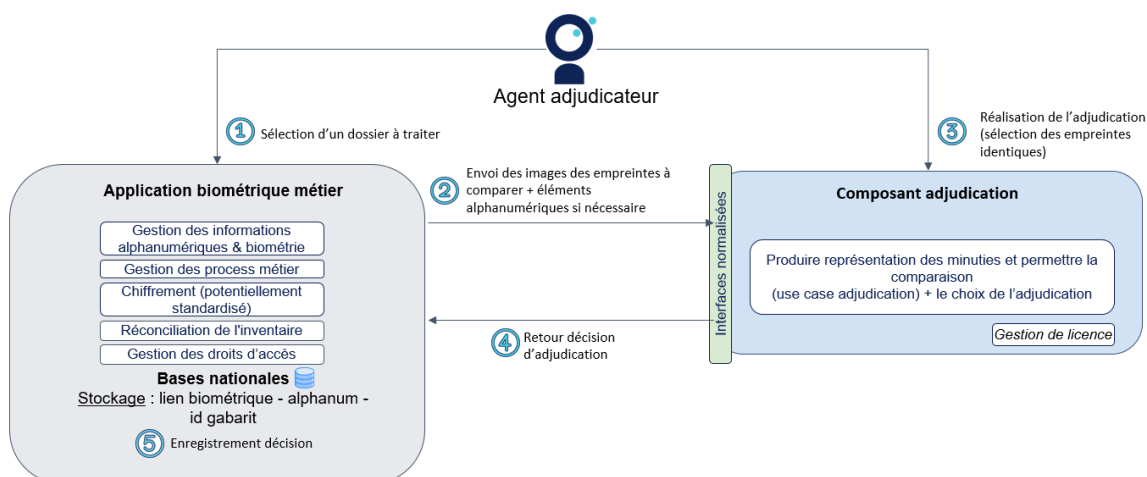


Figure 3: Composant d'adjudication

Le tableau suivant présente la liste des fonctionnalités minimales du composant d'adjudication :

FONCTIONNALITES	FONCTION	DESCRIPTION
Adjudication : Affichage des minuties ou position des yeux Traitement d'image (empreinte, faciale, iris, etc)	Comparaison d'empreintes, faciale ou autres biométries	Un système qui permet une identification biométrique suite à une requête : Processus de décision basé sur la comparaison des données biométrique. Celle-ci permet ensuite de prendre une décision en cas de similitudes de caractéristiques biométriques.

II.6 INTERFACES D'ECHANGE

Dans le cadre de la démarche d'évolutivité voulue par le ministère, la DTNUM a fait le choix de la mise en place d'interfaces d'échange normalisées

- 1- Entre les composants du CBIMI et l'application biométrique métier qui permettent une meilleure stabilité, et une maintenabilité du système en limitant les impacts des évolutions des différents composants du CBIMI sur les applications biométriques métiers. Cette normalisation a pour but de rendre le système plus conforme aux normes industrielles et garantir la pérennité dans un environnement en constante évolution.

Chaque composant du CBIMI dispose d'une interface normalisée et paramétrable permettant aux applications biométriques métiers de les piloter en leur fournissant par exemple un niveau de contrôle, la nature d'une opération (enrôlement, identification...) entre autres.

- 2- Au sein des composants biométriques, les interfaces avec les briques éditeurs sont également normalisées pour limiter les impacts d'un changement d'éditeur ou d'une évolution.

Les interfaces sont dans le périmètre du lot 1.

Par ailleurs, ces interfaces facilitent l'intégration des composants du CBIMI avec des composants éditeurs. Cela permet de maintenir la flexibilité du système et d'assurer une évolution sans perturbation majeure.

Elles ont un rôle de médiateur, en transmettant les requêtes de l'application métier vers le composant de captation. Elles assurent ensuite le traitement des données capturées en les dirigeant vers le noyau biométrique, qui effectue l'analyse nécessaire. Enfin, elles retournent le résultat d'identification généré par le « noyau biométrie » à l'application métier pour une prise de décision (cf. schéma ci-après).

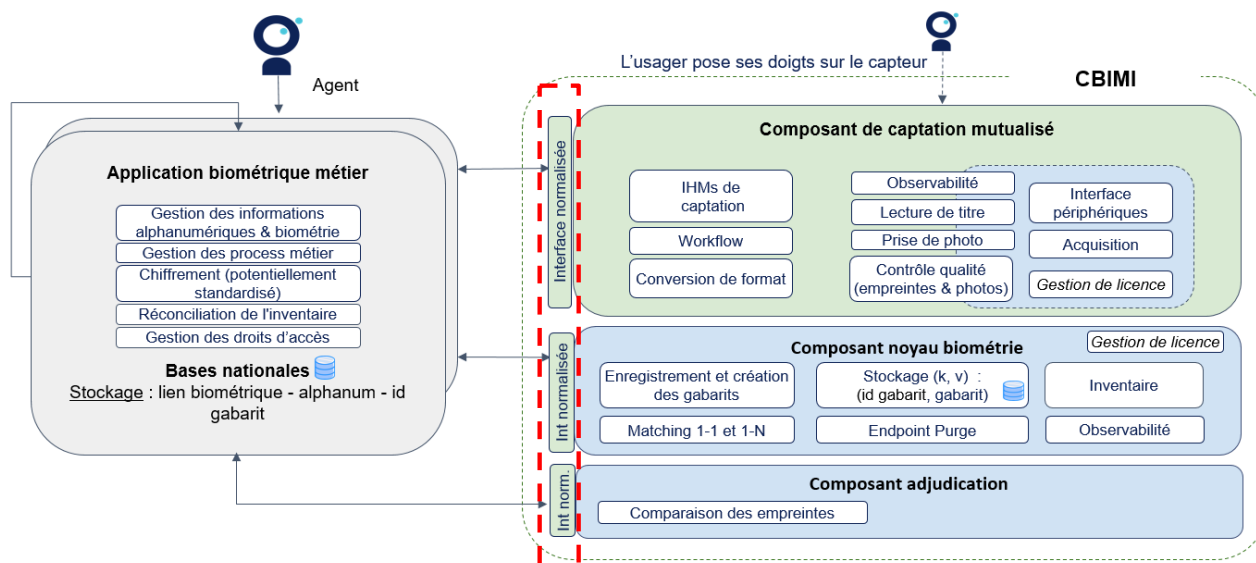


Figure 4: positionnement des interfaces

II.7 MODULE D'OBSERVABILITE

Le CBIMI intègre un outil d'observabilité qui permet de suivre les indicateurs de performance à la fois sur le composant de captation et sur les autres composants (« noyau biométrie » et adjudication).

L'observabilité fait référence à la capacité de surveiller, mesurer et comprendre l'état d'une application en examinant ses sorties, ses journaux et ses indicateurs.

Elle absorbe et étend les systèmes de surveillance et aide les équipes à identifier les causes premières des problèmes.

Au niveau du CBIMI cette fonctionnalité a deux objectifs :

1. Alimenter la plateforme d'observabilité du Bureau de la Fiabilisation des Opérations pour la détection automatique d'anomalies, l'analyse des causes premières et les analyses prédictives.
2. Tracer les actions effectuées par l'utilisateur et l'état des composants éditeurs, pour informer l'utilisateur d'éventuels problèmes et rétrospectivement analyser un problème utilisateur précis sous l'angle fonctionnel. Ces informations pourraient être visualisable via une interface destinée à un administrateur national.

Cet outil a pour vocation d'améliorer la fiabilité du système mis en place dans le cadre du CBIMI. Il doit permettre en outre :

- D'afficher les SLA et leur mesure,
- D'anticiper et prévenir les incidents,
- Gain de temps dans les investigations en cas d'incident,
- Métriques et alertes permettant d'adresser les problèmes utilisateurs (par exemple, page indisponible, nombre de connections anormalement faible, nombre d'utilisations de la fonctionnalité prise de photo, ...)
- Permet de mesurer les impacts de nouvelles fonctionnalités avant de les mettre en production,
- Adapter le dimensionnement du système en fonction de la charge,
- Garantir la conformité et la représentativité des environnements par rapport à la production.

Chaque lot participe à cette fonctionnalité soit au travers des logs, des journaux etc... soit au travers de données enregistrées en base.

II.8 PRINCIPE D'INSTANCIATION

Le principe d'instanciation retenu ici est celui où chaque application métier utilise sa propre instance de chaque composant du CBIMI (hors composant de captation : « CDC ») permettant ainsi de garantir une séparation claire et indépendante des données et des droits d'accès pour chaque application. Cela signifie que chaque application dispose d'un environnement biométrique distinct, isolé des autres applications.

Autrement dit, chaque application (par exemple sur le schéma ci-après, App1 et App2) utilise une instance dédiée du même composant « noyau biométrie ». Ces instances fonctionnent de manière autonome et interagissent avec des bases de données séparées.

II.9 CALENDRIER PREVISIONNEL

Le calendrier suivant est présenté à titre indicatif.

		2025					2026				2027				2028
		T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1
Noyau CBIMI	Enrichissement 2														
	Enrichissement n														
	MVP														
	Enrichissement 1														
POC 1															
Adjudication	MVP														
	Enrichissement 1														
	Enrichissement n														
POC 2															
Connexion avec	APPLI 1														
	APPLI 2														
	N														

Figure 5: Calendrier indicatif

Une première version (MVP) du composant de captation devrait être livrée au second trimestre de 2026.

III. GOUVERNANCE DE L'ACCORD CADRE

La gouvernance, telle qu'illustrée ci-après, s'organise au niveau du projet, pendant la durée du marché. Les différentes instances de gouvernance de l'accord cadre sont illustrés comme suit :

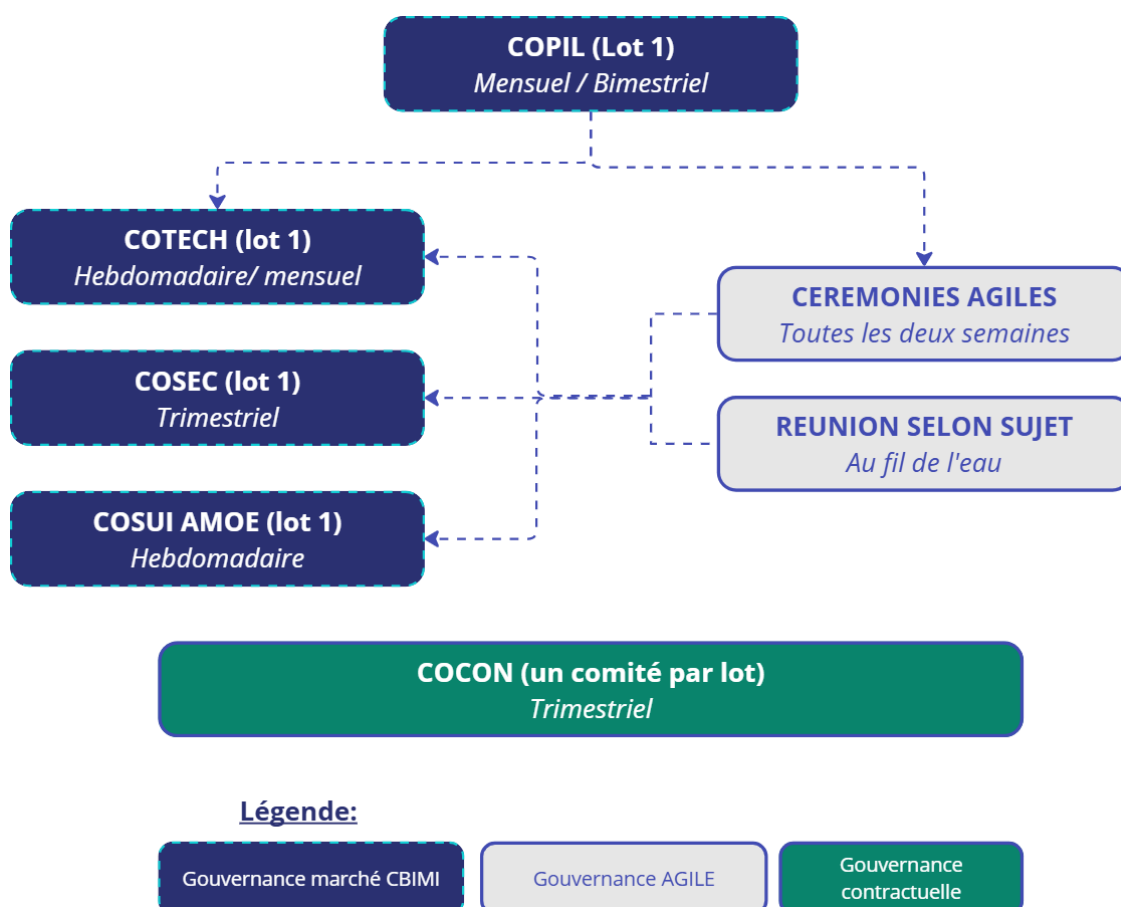


Figure 6: Organisation de la gouvernance

La suite de ce chapitre présente les différentes instances en dehors de celles relatives à la gouvernance Agile qui sont précisées dans les parties en amont.

Le pilotage ne fait l'objet d'aucune prestation individualisée. En tout temps de l'exécution du marché, le titulaire doit intégrer la totalité des charges de pilotage aux prestations sans qu'il puisse réclamer, à ce titre, aucun règlement d'aucune sorte en supplément du prix des prestations tel que fixé à l'annexe financière.

Cette gouvernance est assurée par quatre instances et un point planning spécifique au besoin à l'issue du **comité dans le cadre du Sprint Planning** et pourra évoluer vers un PI (program incrément) si la taille des équipes le nécessite.

III.1 LE COMITE DE PILOTAGE (COPIL)

Des comités de préparation sont organisés autant que nécessaire en vue de la tenue du COPIL.

Les supports et compte rendu sont à la charge du titulaire du lot 1 lorsqu'il participe aux comités.

Comité de pilotage (COPIL)		
Objectif	<p>Le COPIL a pour rôle de fixer les orientations majeures de l'activité confiée au titulaire du marché, de valider les phases de déroulement des travaux, d'assurer les prises de décision stratégiques et d'arbitrer en conséquence les budgets et calendriers. Le COPIL peut être réuni à la demande de l'administration ou du titulaire. Un comité de pilotage exceptionnel peut être convoqué par l'administration à tout moment en fonction des nécessités.</p> <p>Tenue de l'instance en présentiel dans les locaux de l'administration.</p> <p>Chaque fois qu'ils le jugent nécessaire, l'administration ou le titulaire peuvent escalader au niveau du comité contractuel des sujets relevant du CoPil.</p>	
Participants	Administration	Titulaire
	Pôle Biométrie ; La SDAN ou adjoint ; Chef de bureau BADM ou adjoint ; MINUM ;	Lot 1 ; Autres lots (si nécessaire).
Fréquence	Tous les mois en BUILD et bimestriel en RUN	
Ordre du jour	<ul style="list-style-type: none"> - Point d'information générale. - Avancement des prestations commandées. - Livrables de la période écoulée et à venir, état des procès-verbaux de réception. - Point budgétaire en bilatéral avec le titulaire (commandes en cours, facturation émise / payée). - Présenter les indicateurs de qualité de service (délais de réalisation des prestations, de livraison, de résolution des anomalies). - Décisions sur les évolutions éventuelles (après présentation des impacts sur les coûts, le calendrier et les travaux en cours). - Acter du ou des prochains comités. <p>L'administration se réserve le droit d'ajouter à l'ordre du jour tout élément qu'elle jugera utile.</p>	
Support	Ordre du jour détaillé à la charge du titulaire du lot 1.	
Compte-rendu	Relevé de décisions et d'actions à la charge du titulaire du lot 1	

III.2 LE COMITE DE SUIVI MOE (COSUI MOE)

Comité de Suivi MOE (COSUI MOE)		
Objectif	Faire le point sur l'avancement de la réalisation, le contenu et la priorisation des projets tels qu'acté lors du COPIL, faire le rappel du planning des travaux et valider les propositions de modifications de planning, exposées et justifiées (dans le cadre de la démarche Agile, cela correspond à la revue du Backlog).	
Participants	Administration	Titulaire

	Pôle Biométrie ; MINUM.	Lot 1 ; Autres lots (si nécessaire).
Fréquence	1 fois par semaine.	
Ordre du jour	<ul style="list-style-type: none"> - Suivi du planning détaillé, des jalons et des fournitures mutuelles, - Analyse des risques et des problèmes ; identification des actions nécessaires, - Suivi des actions projet, - Suivi du Backlog d'anomalies et d'évolutions, - Date du ou des prochains comités. 	
Support	<ul style="list-style-type: none"> - Présentation détaillée de l'ordre du jour. - Tableau de suivi des actions. - Planning. - Liste du Backlog 	
Compte-rendu	<ul style="list-style-type: none"> - Tableau de suivi des actions mis à jour. - Les décisions et actions à entreprendre par le titulaire ou par l'administration, - Le cas échéant, point nécessitant une décision du COPIL. - Selon accord entre l'administration et le titulaire, la mise à jour du support peut tenir lieu de compte-rendu de réunion. 	

III.3 LE COMITE TECHNIQUE (COTECH)

Comités techniques (COTECH)		
Objectif	Les comités techniques ont pour objet de traiter les sujets techniques et/ou fonctionnels lors de l'exécution des prestations. Ils peuvent également traiter spécifiquement des résolutions des anomalies constatées.	
Participants	Administration	Titulaire
	<ul style="list-style-type: none"> - DTNUM/Pôle Biométrie, - DTNUM/SDAS DevOps, - DGEF/MINUM - DGEF/directions métiers ou directions d'application 	<p>Interlocuteur du titulaire du lot 1 et des autres lots si nécessaires ;</p> <p>Experts fonctionnel, technique ou sécurité ;</p> <p>Toute personne dont la présence est jugée utile selon l'ordre du jour.</p>
Fréquence	1 fois par semaine en BUILD et mensuel en RUN	
Ordre du jour	Points techniques, fonctionnels, d'exploitation ou d'installation à traiter en séance. Plan d'actions.	
Support	<p>Présentation détaillée de l'ordre du jour.</p> <p>Tableau de suivi des actions.</p> <p>État récapitulatif des interventions.</p>	
Compte-rendu	<p>Tableau de suivi des actions mis à jour.</p> <p>Le cas échéant, point nécessitant une décision du comité de projet.</p>	

III.4 LE COMITE DE SECURITE (COSEC)

Comité de sécurité (COSEC)		
Objectif	Le comité de sécurité dans un projet a pour objet de garantir que les aspects de sécurité sont pris en compte tout au long de l'accord cadre. Ce comité assure la gestion des risques liés à la sécurité. Il évalue les risques de sécurité, s'assure de la conformité du PAS , monitore les indicateurs en continue, définit approuve les politiques et mesures de sécurité.	
Participants	Administration	Titulaire
	Pôle Biométrie, MPSSI, RSSI DGEF.	Représentant du titulaire Autres lots (si nécessaire)
Fréquence	1 fois par trimestre	
Ordre du jour	Respect des indicateurs de sécurité (SSI)	
Support	Tableau de bord de sécurité, Rapport d'Audits, Liste des incidents résolus et en cours.	
Compte-rendu	Rapport de suivi de sécurité, Tableau de suivi des actions, Règles et procédures mises à jour, Le cas échéant, point nécessitant une décision du COPIL.	

III.5 LE COMITE CONTRACTUEL(COCON)

Comité contractuel (COCON)		
Objectif	Le titulaire y présente l'avancement contractuel (commandes, paiements, difficultés rencontrées, proposition d'évolution, etc.) des prestations qui lui ont été commandées. Il y présente également tous les indicateurs permettant de suivre l'évolution de l'accord-cadre et des consommations.	
Participants	Administration	Titulaire
	Pôle Biométrie, Chef de bureau BADM, MINUM.et directions métiers ou directions d'applications	Individuel par lot
Fréquence	1 fois par trimestre	
Ordre du jour	Respect des indicateurs de qualité de service	
Support	Reporting SLA.	

	Liste des incidents résolus et en cours.
Compte-rendu	Tableau de suivi des actions mis à jour. Le cas échéant, point nécessitant une décision du COPIL.

Le titulaire s'engage à assurer l'organisation (préparation des supports, organisation logistique, rédaction des comptes-rendus) de l'instance dont il a la charge, à contribuer à la préparation des instances sur demande de l'administration, et à participer aux instances auxquelles il est convié.

IV. SOCLE TECHNIQUE

IV.1 PRINCIPES GENERAUX

IV.2 STRATEGIE D'API SATION

Afin de favoriser l'ouverture et l'évolution du CBIMI, une stratégie d'API sation, alignée avec la stratégie API du cadre de cohérence technique de l'administration, est adoptée et suit les principes suivants :

- orienter l'exposition des services autour des ressources métier ;
- chaque service expose une API unique qui peut servir différents besoins ;
- les API exposées sont autonomes, notamment en termes de gestion de la sécurité et des habilitations ;
- l'ouverture d'une API à un futur partenaire ne doit pas rencontrer de frein technique.

IV.3 SUPERVISION ET MONITORING DE LA SOLUTION CIBLE

Les principes suivants sont respectés par les titulaires :

Disponibilité :

- **garantir un taux de disponibilité** des composants en fonction de leur **criticité métier** et de la catégorie des partenaires (ex : les services de consultation de dossiers doivent être accessibles 24/24 et 7/7 pour les forces de l'ordre) ;
- s'appuyer sur la solution Cloud de l'administration pour assurer la haute disponibilité des composants ;
- configurer les briques techniques (« load balancer », cluster, nombre de réplicas...) pour gérer le traitement des demandes et le passage à l'échelle (scalabilité) ;

Monitoring et supervision :

- **centraliser l'ensemble des logs applicatifs** dans une solution unique type Elastic Stack ;
- mettre en place des sondes sur les composants donnant de la visibilité sur l'état (« healthcheck »).

IV.4 PRINCIPES DE SECURISATION

Les principes suivants sont respectés par le titulaire :

Sécurisation des échanges

- **Encryptions SSL pour tous les échanges** : génération de certificats respectant la norme RGS. Aucun échange non chiffré, même au sein du réseau ministériel, n'est accepté en cible.

Sécurisation des accès

- **Identification systématique des accédants pour chaque service** : tout utilisateur ou application partenaire doit être identifié et des habilitations doivent lui être attribuées. Chaque service doit pouvoir rejeter une sollicitation qui ne possède pas le bon niveau d'habilitation.

Observabilité

- **Tenue d'une piste d'audit** : toute opération est tracée et liée à l'identité de l'accédant qui en est à l'origine, de sorte que le comportement du système global reste observable et que l'administration soit en mesure de détecter des comportements anormaux, même lorsque plusieurs services sont impliqués.

Protection des données

- **Chiffage des données personnelles au niveau du stockage** : quand le besoin est avéré, les données identifiées sont chiffrées en base en se reposant sur les outils de chiffrement inclus dans la solution de stockage.

IV.5 TECHNOLOGIES UTILISEES ET SOCLE DE DEVELOPPEMENT DU TITULAIRE

Les technologies utilisées dans le cadre du CBIMI doivent répondre aux enjeux suivants :

- répondre aux besoins fonctionnels ;
- s'adosser aux expertises de développement déjà présentes ;
- garantir une pérennité acceptable ;
- offrir une opérabilité suffisante et simple en production.

IV.6 CHAINE INDUSTRIELLE DU MINISTERE

Le titulaire est responsable de l'usage par ses personnels (et de ses sous-traitants) des logiciels et des informations utilisées pour la réalisation des prestations dues au titre du présent accord-cadre, et notamment dans le respect du code de la propriété intellectuelle et du secret des affaires.

Hormis les logiciels et plateformes identifiés comme étant fournis par la DTNUM (poste de travail, plateau projet, infrastructure et environnements de développement sur le cloud PI, forges CI et CD), l'ensemble des outils et logiciels nécessaires sont à la charge du titulaire.

Le titulaire est notamment en charge d'approvisionner les licences nécessaires à la réalisation des prestations sur leur environnement.

En cas de perte, destruction ou vol de logiciels et/ou de la documentation afférente, dont l'administration détient le droit d'utilisation, confiés au titulaire, celui-ci est redevable envers elle de leur remboursement à hauteur de leur valeur de remplacement au moment où la perte, la destruction ou le vol est déclaré à l'administration.

L'ensemble des consommables nécessaires au fonctionnement de l'équipe du titulaire et à la réalisation de la prestation sont à la charge du titulaire.

IV.7 DEVELOPPEMENTS CHEZ LE TITULAIRE

L'infrastructure logicielle et matérielle est fournie par le titulaire du lot 1, au titre de la prestation de « initialisation et prise de connaissance »

Les serveurs doivent être hébergés en Europe, et la solution « Cloud » doit être compatible avec OpenStack (HP) et éventuellement OpenShift.

La plateforme de développement à distance du titulaire doit également être accessible à distance par l'administration.

Le titulaire ou ses co-traitants et/ou sous-traitants ne doivent utiliser aucun outil qui ne ferait pas partie des outils listés ci-dessus. Le cas échéant, les demandes de dérogation seront à soumettre obligatoirement et en amont de l'utilisation au CTO de la sous-direction des applications numériques.

Ces obligations d'usage et restrictions s'appliquent également aux composants validés par la sous-direction des applications numériques.

Par principe, seront recherchés l'utilisation d'outils en open-source et installables on premise sur les infrastructures de l'administration.

Les outils de la chaîne industrielle utilisée par l'administration font l'objet d'exigences standardisées.

L'accès est contrôlé à travers une procédure d'identification (nom d'utilisateur + mot de passe). Chaque utilisateur dispose d'un profil définissant son niveau d'habilitation.

Le titulaire respecte les consignes d'utilisation de l'outil, fournies par l'administration le titulaire signale, au plus vite, à l'administration tout problème d'indisponibilité des outils.

L'exploitation des données enregistrées lors de l'usage de ces outils permette de produire les indicateurs contractuels de volumétrie et de qualité de la prestation.

IV.8 PILES LOGICIELLES

L'administration a défini sa chaîne industrielle de « delivery » et de support, les titulaires devront utiliser les outils choisis par l'administration (liste pouvant être réactualisée).

Elle est constituée des éléments suivants :

Nom	Outil
Ansible	Outil d'infrastructure as code, qui permet de définir la configuration d'une VMs (installation de packages, configuration de l'OS etc...) via du code, donc automatisable et versionable
Client git	Repository (dépôt code source)
Consul	Outil d'annuaire DNS, de service discovery et une base de donnée clé valeur qui implémente un algorithme de consensus (RAFT), permettant de stocker données avec un besoin critique de cohérence
Cucumber	Tests BDD
Cypress	Tests
Docker	Outil de conteneurisation léger qui permet de créer, déployer et gérer des applications dans des conteneurs isolés
JIRA et TULEAP	Gestion du backlog et du flux de travail des US Gestion des anomalies et autres tickets
FIGMA	Outil collaboratif d'exploration produit, de design et de Réalisation de maquettes
GLPI / MINITIL	Gestion des demandes et des signalements
Squash TM	Gestion des référentiels de tests et suivi de campagne de tests
Resana	Gestion documentaires et espace collaboratif
Apache JMeter	Outil de tests de performance d'applications et de serveurs
Zed !	Conteneurs chiffrés pour sécuriser le transport de fichiers
Sophos / ClamAV ou antivirus en vigueur au MI	Antivirus
JDK	Développement
Eclipse	Développement

Entreprise Designer	Modélisation de base de Données
Gatling	Outil de tests de performances, basé uniquement sur du code, facile à intégrer dans une CI
GITLAB	Plateforme DevOps open source qui s'appuie sur le logiciel de gestion de versions Git. Elle permet de créer, tester et déployer des logiciels de manière collaborative.
InelliJ	Outil de développement
Jaeger	Outil de visualisation de trace des applications
KeyCloak	Gestion des identités et des accès
Kibana/Elasticsearch/ Fluentd	Solutions permettant d'ingérer, d'indexer, de parcourir des logs et de définir des dashboards
Entreprise Designer	Modélisation de base de Données
PostgreSQL	Base de données relationnelle
Maven	Gestionnaire de dépendance, construction et packaging de projet
MongoDB	Base de données no-sql
EDGE, Firefox, Chromium	Navigateurs
WinSCP	Client sftp graphique
AWX	L'automatisation de tâche autour de l'intégration Continu et du déploiement continu
Gitlab CI	L'automatisation de tâche autour de l'intégration Continu et du déploiement continu
Nexus	Stockage et mise à disposition des différentes versions des modules du projet
Pgpatroni	Outil de mise en haute dispo de postgresql
Prometheus/Grafana/ Alert-Manager	stack permettant de monitorer l'état des VMs (CPU, RAM, IO, process en cours etc...), de définir des alertes et de visualiser ces états via des dashboards
Redis	Base de donnée clé valeur pour les accès en lecture écriture fréquent (exemple de cas d'usage : stockage de session pour des applications web distribuées)
Selenium	Test de logiciel automatisé
J Unit, PHP Unit	Tests unitaires
Centreon	Supervision
Openshift V3.11	Permet de déployer des projets dans des container
Ref APP (Canel)	Cartographie applicative
S3	Stockage objet
SonarQube	Qualimétrie en continu
Suite Bureautique	Suite Libre Office
WEBCONF ou COMU	Outil de Conférence
Tchap	Messagerie instantanée
Terraform	Outil d'infrastructure as code, qui permet de définir une infrastructure (VMs, réseaux etc...) via du code, donc automatisable et versionable

Les versions de référence sont définies dans le cadre de cohérence technique de l'administration (en annexe). Elles sont susceptibles d'évoluer pendant la durée du marché.

V. EXIGENCES COMMUNES À L'ENSEMBLE DES PRESTATIONS

V.1 EXIGENCES GENERALES

Référence	Description
EG1	Le titulaire met en place une structure adaptée au projet, selon la méthodologie Agile. L'équipe associée au projet est dédiée au programme et dimensionnée afin de conduire dans les délais, et avec le niveau de qualité requis, les prestations demandées.
EG2	Afin de coordonner toutes les actions nécessaires à la bonne exécution du projet et d'assurer sa pleine mission de conseil, le titulaire dispose dans ses ressources internes, d'experts dans chacun des domaines abordés par le programme. Le cas échéant, le titulaire doit être capable de mobiliser les ressources nécessaires.
EG3	Le titulaire s'engage à informer au plus tôt l'administration de tout changement de personnel au sein de son équipe. En tout état de cause, le changement de personnel ne peut impacter la bonne marche du programme tant en matière de délais que de résultats.
EG4	Le titulaire s'engage à effectuer son devoir de conseil et d'alerte vis-à-vis de l'administration, de même, l'administration s'engage à respecter son devoir d'information et de collaboration avec le titulaire.
EG5	L'administration se réserve le droit de conduire des audits à titre préventif ou en cas de non-respect des dispositions de qualité liées au système dont le titulaire assure la maintenance ou les évolutions, ou pour les procédés mis en œuvre pour le développer ou le vérifier, et plus généralement l'administration se réserve le droit de diligenter des audits sur tout ou partie des prestations réalisées ainsi que sur les méthodes utilisées.
EG6	A la suite d'une demande d'audit formulée par l'administration, le titulaire lui donnera accès sans restriction aux locaux où se déroulent les prestations (si hors site de l'administration), et à toutes les informations concernant la prestation.

V.2 EXIGENCES SUR LA DOCUMENTATION

Référence	Description
ED1	<p>Les livrables sont des documents rédigés en langue française et transmis à l'administration obligatoirement sous format numérique.</p> <p>La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Les titulaires fournissent à l'administration les livrables identifiés pour chaque prestation, dans une version stable.</p>

Référence	Description
ED2	Tout document fourni à l'administration par le titulaire à titre provisoire ou définitif comportera les informations suffisantes pour identifier sans ambiguïté ce document, sa version (Vi.j), la date de cette version, son type (compte-rendu de réunion, support de formation, documentation...), son degré d'achèvement, son niveau de vérification et la version de l'application avec laquelle il est cohérent. Cette exigence s'applique à la documentation en ligne.
ED3	Toute modification apportée sur un document élaboré par le titulaire et déjà livré à l'administration dans une édition précédente sera identifiée explicitement dans le texte de la nouvelle édition du document et tracée dans un historique.
ED4	<p>Les informations contenues dans la documentation définitive fournie par le titulaire devront être à jour, complètes, cohérentes et exemptes de toute annotation provisoire. Elles devront éviter toute redondance injustifiée.</p> <p>Le titulaire apportera la preuve de ses contrôles par la mention en tête de chaque document des noms et qualités des relecteurs et de la date de validation par ceux-ci.</p>
ED5	<p>La transmission de cette documentation se fera telle que définie dans les plannings, et sera tracée lors des comités ad-hoc.</p> <p>Le document désigne les destinataires.</p>
ED6	<p>Le nombre de documents à produire dans le cadre du marché et selon les travaux à réaliser s'avère important (Product Backlog + les User Stories), dossier de conception technique, guide utilisateurs, notes diverses, manuels d'exploitation, DAT, etc.).</p> <p>Par conséquent, le titulaire doit adopter une démarche permettant d'optimiser la phase de relecture des documents et de validation des documents.</p> <p>Il met en place à cet effet un espace partagé accessible par les différentes personnes désignées par l'administration.</p> <p>Les principes suivants devront être respectés :</p> <ul style="list-style-type: none"> • chaque nouveau document à produire passe par : <ul style="list-style-type: none"> ○ le respect du formalisme et de la structuration du document définis par ou avec l'administration ; ○ une première étape de validation sur le plan, le contenu détaillé et la forme du document (revue du sommaire, accord sur le contenu) ; ○ le cas échéant, pour les documents volumineux, une deuxième étape à mi-chemin pour contrôler l'état d'avancement du document et en faire une première lecture ; ○ une ultime étape de validation, une fois le document terminé du point de vue de son rédacteur ; • pour les documents faisant simplement l'objet de modifications (suite aux évolutions du système), le titulaire fait en sorte que les modifications apportées soient identifiables sans ambiguïté (mode correctif de MS Word par exemple) ; • les documents dans une version définitive sont distingués des documents de travail. Ces derniers d'une durée de vie limitée à une phase transitoire des travaux ont pour vocation de produire un document définitif par création ou modification. Seule l'administration statue sur le caractère définitif d'un document. Sa version antérieure peut éventuellement être sauvegardée ;

Référence	Description
	<ul style="list-style-type: none"> l'ensemble des documents sont impérativement stockés dans un espace proposé et tenu à jour par le titulaire et accessible aux personnes désignées par l'administration ; tout livrable (SFD, dossier de conception technique, guide utilisateurs, notes diverses, manuels d'exploitation, etc.) est obligatoirement transmis dans un format bureautique (type MS Word) imprimable et modifiable, en sus d'une livraison sous une autre forme (si applicable). <p>Le titulaire s'assure également que les évolutions / modifications ou ajouts de documents au sein de l'espace partagé puissent générer une alerte auprès des personnes de l'administration concernées afin de les informer.</p> <p>Le titulaire peut être force de proposition sur le sujet afin d'améliorer davantage ce dispositif, et de lisser dans la mesure du possible la charge inhérente de validation à réaliser de la part de l'administration.</p>
ED7	<p>Chaque titulaire définit et exécute un processus de contrôle préalable en interne avant toute livraison à l'administration, permettant de vérifier la satisfaction des exigences requises comme définies ci-dessous :</p> <ul style="list-style-type: none"> Exigences de forme : <ul style="list-style-type: none"> conformité aux modèles types mis en place par l'administration et disponibles dans des documents de référence, ou, à défaut, des modèles types proposés par chaque titulaire dans leur offre et validés avec l'administration ; conformité avec les spécifications et les objectifs de la maquette ou du prototype ; exhaustivité, mise à jour, traçabilité, réutilisabilité du support ; exactitude, lisibilité, cohérence intrinsèque et avec les autres productions documentaires ; rédaction, orthographe, grammaire ; nommage (règles définies ci-dessus, si non-respect des règles définies conjointement avec l'administration) ; toute(s) autre(s) exigence(s) précisée(s) dans le bon de commande ; Exigences de fond : <ul style="list-style-type: none"> pertinence des analyses, expertises développées, au regard des enjeux exprimés par l'administration ; en cas de développement, qualité du code fourni, des rapports de tests, des commentaires et de la documentation associée, ainsi que tout élément indispensable à la bonne compréhension et au fonctionnement opérationnel de la fonction/application/service concerné(s) ; valeur ajoutée des propositions de scénarii et de solutions faites en résultat des études commandées par l'administration ; argumentation claire et pertinente des solutions proposées ; couverture (fonctionnelle, technique, etc.) de l'ensemble des points et spécifications à traiter, par rapport à l'expression des besoins de l'administration et à l'état de l'art ; démonstration de la prise en compte des spécificités du besoin exprimé par l'administration par la formalisation de scénarii, solutions,

Référence	Description
	<p>spécifications personnalisées ;</p> <ul style="list-style-type: none"> ○ toute autre exigence précisée dans le bon de commande. <p>Pour chaque livrable documentaire, l'administration évalue la qualité de la livraison selon les exigences ci-dessus et les modalités de réception et vérification précisées dans les documents du présent accord-cadre. Un manquement à cette nécessité de qualité peut motiver une décision d'ajournement par l'administration dans les conditions définies au CCAP.</p>
ED8	Le titulaire assure la gestion de la documentation qui lui est confiée, et sa confidentialité : des sauvegardes sont réalisées et les accès sont strictement limités aux personnes habilitées.
ED9	<p>Le titulaire utilise les outils de cryptage compatibles avec ceux de l'administration pour les documents à accès restreint (DAT, DAA, etc.) définis avec l'administration. Les outils utilisés sont :</p> <ul style="list-style-type: none"> • Zed projet pour le programme et administré par la maîtrise d'œuvre ou son représentant.

V.3 EXIGENCES SUR LA CONDUITE DES PRESTATIONS

Référence	Description
ECP1	<p>Le titulaire assure le suivi détaillé de toutes les actions relatives au présent marché.</p> <p>Il fournit à l'administration l'ensemble des indicateurs de suivi lui permettant d'avoir pleinement connaissance de l'avancement du projet, des actions menées et des actions restantes à mener.</p>
ECP2	Le titulaire veille à mettre à jour le suivi d'actions et à le rendre disponible de manière dématérialisée à la demande de l'administration.
ECP3	À chaque comité contractuel, le titulaire fournit à l'administration un tableau de bord complet d'avancement de l'ensemble des prestations du présent CCTP.
ECP4	<p>Le titulaire propose les outils de suivi de projet (tableau de suivi des travaux et des risques, tableau de bord des livrables, indicateurs, autres) qui doivent être validés par l'administration lors de la phase de lancement.</p> <p>Il devra fournir à l'administration un tableau de bord tous les 2 mois.</p>
ECP5	<p>L'administration fournit l'hébergement et les licences des outils de gestion du <i>backlog</i> et de la documentation de développement. Elle administre ces outils.</p> <p>Le titulaire l'assiste dans l'administration et gère ces outils pour l'ensemble des acteurs du projet.</p> <p>Les outils retenus pour le développement fonctionnel sont Jira d'Atlassian (Expression de besoin ou dossier de conception fonctionnelle/Story Mapping, SFD).</p> <p>En parallèle, une GED projet classique de l'administration (RESANA) sera mise en place dès le début du projet pour la gestion de marché, et pour les documents sensibles d'architecture.</p>
ECP6	Le titulaire s'engage à participer aux structures de pilotages et de revues permettant de s'assurer du respect des exigences de l'administration en matière de coût, de délai

Référence	Description
	et de qualité.
ECP7	<p>Les tableaux de bord de suivi des prestations sont élaborés sur la base d'un modèle proposé par chaque titulaire.</p> <p>Ce modèle doit être validé par l'administration qui pourra en demander des évolutions auxquelles le titulaire devra se conformer. Celui-ci présentera au minimum :</p> <ul style="list-style-type: none"> • pour les projets en cours de conception/développement : <ul style="list-style-type: none"> ○ l'état d'avancement de développement par rapport au calendrier ; ○ le niveau de vélocité atteint ; ○ le bilan des dernières livraisons ; ○ le nombre d'anomalies et l'état d'avancement de résolution. • pour la maintenance corrective : <ul style="list-style-type: none"> ○ nombre d'incidents réceptionnés mentionnant par type (bloquant, prioritaire, non prioritaire) ; ○ nombre de corrections d'incidents par type livrées et délais de livraison ; ○ nombre d'incidents en cours de traitement par type et date ; • pour la maintenance évolutive : <ul style="list-style-type: none"> ○ demandes d'évolutions reçues, chiffrées, commandées, en cours de réalisation, réalisées, livrées, délais de livraison, motifs d'éventuels retards ; ○ bilan des dernières livraisons ; • pour les autres prestations : <ul style="list-style-type: none"> ○ état d'avancement et/ou bilan. <p>Ces tableaux de bord sont présentés en comité dédié et sont régulièrement tenus à jour par le titulaire.</p> <p>Pour le suivi de la qualité de traitement des demandes d'intervention ou de résolution des incidents (anomalies applicatives) les indicateurs fournis sont mis à jour toutes les semaines.</p>

V.4 EXIGENCES SUR LA GOUVERNANCE

Référence	Description
EGV1	<p>Le titulaire désigne un interlocuteur unique pour le suivi du marché. Il est le garant du respect :</p> <ul style="list-style-type: none"> • de l'exécution des prestations ; • du respect des niveaux de services ; • de l'ensemble des exigences du marché ; • du respect des normes, standards, méthodes et démarches mises en place dans le cadre du marché. <p>Une attention particulière sera portée sur l'organisation de la gouvernance dans le</p>

Référence	Description
	premier mois de mise en œuvre du marché, notamment sur la mise en place d'un plan d'assurance qualité partagé par l'ensemble des acteurs.
EGV2	En cas de départ de l'interlocuteur unique pour le suivi du marché du titulaire, la période de recouvrement pendant laquelle le partant forme la nouvelle personne pressentie pour la conduite du projet doit être au minimum d'un mois calendaire.
EGV3	Dans le cas d'un problème critique, identifié par l'administration dans ses relations avec le titulaire, ou dans le fonctionnement du système pour lequel l'administration n'obtient pas satisfaction de la part du directeur de projet du titulaire, le titulaire fera en sorte de mobiliser et de mettre en contact sa hiérarchie (par exemple son directeur général) avec le responsable de l'administration concerné dans les 5 jours ouvrés à compter de la date de notification du problème par l'administration.

V.5 EXIGENCES SUR LES RESSOURCES DU TITULAIRE

Référence	Description
ERT1	Le titulaire doit disposer de ressources suffisantes et ayant les compétences et l'expérience requises pour couvrir l'ensemble des prestations de son lot. Les technologies sont, au minimum, celles qui figurent dans la liste des applications du SI existant.
ERT2	Chaque titulaire communique à l'administration, à sa demande, les noms, titres et coordonnées professionnelles des personnes physiques en charge de l'exécution des prestations.
ERT3	<p>La séniorité des profils est définie comme suit :</p> <ul style="list-style-type: none"> • profil junior : jusqu'à trois (3) ans d'expérience, disposant d'une formation sur le domaine de compétence demandé ; • profil confirmé : de trois (3) à six (6) ans d'expérience ; • profil senior : plus de six (6) ans d'expérience, avec des expériences d'expertise dans le domaine concerné ; • profil expert : plus de dix (10) ans d'expérience, expertise reconnue par ses pairs, cursus de formation continue et certifications, publications et animation de communauté. <p>La séniorité des développeurs est définie comme suit :</p> <ul style="list-style-type: none"> • développeur junior : jusqu'à trois (3) ans d'expérience, disposant d'une formation aux technologies demandées ; • développeur confirmé : de trois (3) à six (6) ans d'expérience ; • développeur senior / « tech lead » : plus de six (6) ans d'expérience, ayant des domaines d'expertise dans les technologies demandées et de l'expérience en tant que « tech lead ». <p>L'expertise se justifie par une formation et une expérience significative dans le domaine d'expertise concerné. Tous les intervenants doivent justifier d'a minima une première formation ou une première expérience dans l'agilité. Les titulaires sont responsables et assurent le plan de développement des compétences de leurs équipes de manière à maintenir un fort niveau d'excellence et une forte motivation.</p>
ERT4	Pour chacune des prestations du marché, les titulaires respectent impérativement les niveaux de séniorité fixés au début de chaque partie dédiée du présent document.

Référence	Description
	<p>Une équipe projet doit être stable et les changements d'acteurs doivent être limités et sans impact sur le déroulement du projet.</p> <p>Le nombre de remplacements d'intervenants à l'initiative du titulaire doit être inférieur à 4%.</p> <p>Ainsi le titulaire s'assure de la disponibilité des intervenants pendant la durée du développement d'une fonctionnalité ou d'une brique transverse. A l'exception d'un cas de force majeure, il n'est pas accepté de remplacement d'intervenant pendant le développement d'une fonctionnalité ou d'une brique.</p>
ERT5	<p>Chaque remplacement doit être organisé de manière à limiter l'impact sur le déroulement du projet. Le titulaire doit s'assurer d'un recouvrement pendant au moins trois semaines entre l'intervenant sortant et l'intervenant entrant.</p> <p>Pour les profils participants aux itérations de développement (équipe du lot 1), le nombre de jours de recouvrement entre le profil sortant et le profil entrant doit être de deux (2) itérations.</p> <p>Les recouvrements ne donnent lieu à aucune demande de règlement d'aucune sorte (seul un profil sur les deux est facturé).</p>
ERT6	<p>Le titulaire s'engage dès lors que son équipe est en place et convient à l'administration, à conserver celle-ci (sauf cas de force majeure ou démission du collaborateur) pendant toute la durée du marché.</p>
ERT7	<p>En tout état de cause et en cas de départ d'un collaborateur du titulaire, celui-ci tiendra informée l'administration au plus tôt et justifiera de son départ.</p>
ERT8	<p>En cas de départ du collaborateur, le titulaire s'engage à le remplacer par une personne au minimum de qualification identique ou supérieure et possédant toutes les compétences en lien avec le marché.</p>
ERT9	<p>Chaque remplacement doit être organisé de manière à limiter les effets sur le déroulement du projet. Le titulaire doit s'assurer d'un recouvrement pendant au moins un mois entre l'intervenant sortant et l'intervenant entrant.</p> <p>Les recouvrements ne donnent lieu à aucune demande de règlement d'aucune sorte (seul un profil sur les deux est facturé).</p>
ERT10	<p>Les CV de tout nouvel intervenant en cours de marché doivent être soumis à l'approbation de l'administration.</p>
ERT11	<p>Dans le cas d'une insuffisance ou d'un manquement dûment constaté par l'administration d'un intervenant du titulaire, d'un commun accord, ce dernier pourvoit à son remplacement en satisfaisant au profil requis avec la remise à niveau nécessaire sans coût supplémentaire pour l'administration dans un délai maximal d'un (1) mois.</p>
ERT12	<p>Les intervenants doivent être localisés en Europe</p>

V.6 EXIGENCES SUR LES MOYENS TECHNIQUES ET SUR LA COHERENCE DE L'ARCHITECTURE TECHNIQUE GLOBALE DU SYSTEME D'INFORMATION

Référence	Description
EMT1	<p>Le titulaire s'engage, dès le début du marché, à assurer la maintenance du CBIMI dans les environnements techniques qui prévalent à leur fonctionnement.</p> <p>Il est entendu que l'administration se réserve le droit de faire évoluer ces exigences en cours de marché, notamment lorsque celles-ci font référence à des solutions techniques spécifiques.</p>
EMT2	<p>Tout composant développé ou nécessaire au bon fonctionnement ou à la compilation des composants développés spécifiques pour le compte de l'administration fait l'objet d'une cession de droit conformément aux clauses relatives au droit de la propriété intellectuelle du CCAP.</p>
EMT3	<p>Conformément aux stipulations du CCAP, l'administration détient l'ensemble des droits de propriété intellectuelle du référentiel des développements. À cet égard, elle doit être en mesure de reconstituer la mémoire des différentes versions des composants applicatifs. L'administration est en mesure de demander un retour à une version antérieure d'un développement. Pour ce faire, tout changement dans un fichier (commit) identifie la nature de la modification qu'il porte.</p>
EMT4	<p>Les tests sur la qualité du code, les tests unitaires et les scénarios de tests sont indissociables du code source et des livrables. Le prestataire garantit leur exécution avant tout livrable. Le titulaire systématise les balises permettant aux équipes de recette d'automatiser les tests, en particulier les tests de non-régression.</p> <p>Le « nombre de fonctionnalités couvertes par des tests automatiques/ nombre total de fonctionnalités » doit être supérieur à 80%.</p>
EMT5	<p>L'environnement de développement, comme tout environnement applicatif, dispose d'un document d'architecture technique, d'une procédure technique d'installation et d'exploitation.</p> <p>Elle permet la gestion et autorise le suivi de l'avancée de l'en-cours avec les versions des composants applicatifs.</p> <p>Elle est porteuse d'une mise en œuvre rigoureuse de l'organisation de projet et particulièrement la mise en place de rôles précis (architecte, développeur, intégrateur, <i>Scrum master</i>, etc.)</p>
EMT6	<p>Le titulaire s'assure, pour l'ensemble des outils logiciels du système d'informations, qu'il adopte des principes d'architecture et une démarche qui soient cohérents sur l'ensemble du SI. À cet effet, il produit des dossiers d'architecture technique communs et transverses. Il assure en permanence le respect de l'état de l'art en matière d'architecture technique du SI.</p>
EMT7	<p>Le titulaire s'engage à se conformer à la charte graphique en vigueur au sein de l'administration (application du DSFR – Design System de l'Etat) pour tout ce qui relève des interfaces utilisateurs et traduites aujourd'hui dans deux bibliothèques de composants.. Il peut être force de proposition sur l'ergonomie et s'assure de la cohérence globale de cette ergonomie sur l'ensemble des IHM du SI.</p>
EMT8	<p>Le titulaire s'engage, pour tout nouveau projet, à réaliser des développements en conformité avec le référentiel RGAA 4 (https://accessibilite.numerique.gouv.fr/).</p>

V.7 EXIGENCES SUR LES VERIFICATIONS ET CONTROLE QUALITE

Référence	Description
EV1	Tout produit ou document résultant d'une tâche et faisant l'objet d'une livraison à l'administration fait l'objet d'un contrôle qualité de la part du titulaire. Ce contrôle est explicitement intégré à la livraison. Il prévient toute régression fonctionnelle ou technique.
EV2	Les différents essais conduits sur le système par le titulaire seront tracés de manière à déterminer la couverture fonctionnelle de ses tests et des spécifications qui s'y rapportent.
EV3	La description et le résultat des actions de vérification conduites par le titulaire seront consignés dans un dossier réservé à cet effet et soumis à la validation par l'administration pour acceptation de la livraison.
EV4	Le « nombre d'US validées / nombre de US planifiées » sur un incrément doit être supérieur à 85%

V.8 EXIGENCES SSI

Référence	Description
ESSI1	Le titulaire se conforme aux PSSI applicables et en vigueur au sein de l'administration.
ESSI2	<p>À l'issue d'une analyse de risque au sens EBIOS que serait amenée à réaliser l'administration sur la plate-forme, le titulaire s'engage à mettre en œuvre toutes les remédiations prescrites par cette analyse de risque. Le cas échéant, ces actions de remédiations sont réalisées dans le cadre de prestations de maintenances adaptatives (sauf en cas où celles-ci s'apparentent à des lacunes de développement et du non-respect de la part du titulaire des PSSI applicables).</p> <p>Dans tous les cas, le titulaire s'assure que les actions de remédiations soient faites sans détériorer la capacité de production fonctionnelle.</p> <p>Les outils déployés actuellement sur le <i>tenant</i> du <i>cloud</i> PI sont homologués au sens EBIOS. Cette homologation doit faire l'objet d'une révision à chaque intégration de nouveaux applicatifs, soit sur un dossier d'analyse d'écart, soit lors d'une procédure complète d'homologation. La démarche d'homologation retenue à ce jour sur le <i>cloud</i> PI est une démarche renforcée.</p> <p>Le titulaire devra mettre en œuvre toutes les remédiations identifiées résultantes des commissions d'homologation.</p>
ESSI3	<p>Le titulaire doit traiter les alertes de sécurité transmises par l'entité responsable ou le responsable de la sécurité du CBIMI.</p> <p>Il doit être force de conseil sur tout patch de sécurité disponible et à mettre en œuvre sur son périmètre.</p>

V.9 EXIGENCES SUR LA RESOLUTION DES ANOMALIES

Référence	Description																				
ERDA1	<p><u>La criticité des anomalies est définie de la manière suivante :</u></p> <p>On distingue les niveaux d’anomalies suivants :</p> <ul style="list-style-type: none">• anomalie bloquante : bloque le fonctionnement du produit. Tout incident produisant l’altération de données ou qui interdit l’accès normal aux données (en lecture et/ou en écriture), ou qui rend impossible l’utilisation normale d’une fonction, de façon rédhibitoire et non contournable par l’administration sans intervention du titulaire. Est reproductible et le processus de reproduction peut être décrit ;• anomalie majeure : interdisant la mise en œuvre d’une ou plusieurs fonctionnalités du produit, sans qu’il existe de solution de contournement acceptable par les utilisateurs en termes de coût et d’organisation. Est reproductible et le processus de reproduction peut être décrit ;• anomalie mineure : anomalie portant sur une ou plusieurs fonctionnalités, n’empêchant pas leur fonctionnement et ne produisant pas d’altération de données ou des résultats, mais rendant l’usage des fonctionnalités plus compliquée et l’augmentation des temps de traitement. Ce type d’anomalie implique soit la correction de l’anomalie soit la mise en œuvre d’un moyen de contournement pouvant être mis en œuvre par un utilisateur pour parvenir au résultat attendu.																				
ERDA2	En cas de désaccord sur la qualification de l’anomalie entre l’administration et le titulaire, le niveau de gravité qui est retenu est celui proposé par l’administration.																				
ERDA3	<p>Les délais de correction des anomalies sont mentionnés dans le tableau ci-après et courent à partir de la remontée de l’incident par l’administration et ce par tout canal approprié (téléphone, mail ou via les fiches « incident » sur l’outil de suivi des incidents, retenu par l’administration). La correction est soit définitive, soit une solution de contournement est mise en place par le titulaire pour pallier le dysfonctionnement. Les jours ouvrés sont tous les jours du lundi au vendredi compris, à l’exception des jours fériés légaux.</p> <p>Les heures ouvrées sont fixées sur les tranches horaires suivantes : de 08h30 à 18h30.</p> <p>Les plages d’ouverture de service étendues : en HNO : le samedi, le dimanche et jours fériés de 08H30 à 18h30, la nuit de 18h30 à 08H30.</p> <table><tr><th>Type d’anomalie</th><th>Anomalie Bloquante</th><th>Anomalie majeure</th><th>Anomalie mineure</th></tr><tr><td>Délai de correction</td><td>1 jour ouvré</td><td>2 jours ouvrés</td><td>Au cours de l’itération suivante</td></tr></table> <table><tr><th>Catégorie d’incident</th><th>Bloquant</th><th>Majeur</th><th>Mineur</th></tr><tr><td>Temps de réponse</td><td>Une (1) heure ouvrée</td><td>Quatre (4) heures ouvrées</td><td>Un (1) jour ouvré</td></tr><tr><td>Solution de contournement</td><td>0,5 jour ouvré</td><td>Deux (2) jours ouvrés</td><td>Dix (10) jours ouvrés</td></tr></table>	Type d’anomalie	Anomalie Bloquante	Anomalie majeure	Anomalie mineure	Délai de correction	1 jour ouvré	2 jours ouvrés	Au cours de l’itération suivante	Catégorie d’incident	Bloquant	Majeur	Mineur	Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré	Solution de contournement	0,5 jour ouvré	Deux (2) jours ouvrés	Dix (10) jours ouvrés
Type d’anomalie	Anomalie Bloquante	Anomalie majeure	Anomalie mineure																		
Délai de correction	1 jour ouvré	2 jours ouvrés	Au cours de l’itération suivante																		
Catégorie d’incident	Bloquant	Majeur	Mineur																		
Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré																		
Solution de contournement	0,5 jour ouvré	Deux (2) jours ouvrés	Dix (10) jours ouvrés																		

Référence	Description				
		En cas d'incident signalé avant 12h : remise en état dans la journée. En cas d'incident après 12h : remise en état pour le lendemain avant 12h			
	Résolution par une solution pérenne	Cinq (5) jours ouvrés	Dix (10) jours ouvrés	Vingt (20) jours ouvrés	
<p>NB : dans le cas d'un incident bloquant, la signalisation est réalisée par téléphone ou un envoi de courriel au titulaire.</p> <p>Les délais exprimés courent à compter de la notification de l'incident par l'administration.</p>					
ERDA4	Le titulaire doit inclure dans chaque itération des corrections de bugs et la réduction de la dette technique ou sécuritaire.				
ERDA5	La part de cette activité corrective ne dépasse pas en story points 20% du contenu de l'itération. Si la part de correction des anomalies d'une itération courante est inférieure à 20% du contenu d'une itération suivante, la correction des anomalies mineures d'une itération courante est effectuée dans l'itération suivante et ne donne pas lieu à une contrepartie financière.				
ERDA6	La correction des anomalies bloquantes et majeures se fait, sans contrepartie financière, dans les délais indiqués dans le tableau ci-dessus sauf exception consentie par l'administration.				
ERDA7	Lorsque le nombre d'anomalies (bloquante, majeure ou mineure) devient trop important (anomalies hors délais), le titulaire élabore un plan de résorption des anomalies et assure d'une itération, dédiée à la correction d'anomalies, sans contrepartie financière de la part de l'administration.				

VI. DISPOSITIONS COMMUNES A L'ENSEMBLE DES PRESTATIONS

VI.1 LIEUX D'EXECUTION ET TELETRAVAIL

Les prestations s'exécutent principalement dans les locaux des titulaires qui doivent obligatoirement se **situer en Europe**.

Les réunions ou ateliers de travail se déroulent dans des locaux de l'administration et exceptionnellement peuvent avoir lieu dans des locaux mis à disposition par le titulaire.

L'infrastructure logicielle et matérielle, notamment les plateformes le « Cloud PI », est fournie par l'administration.

Le titulaire met en œuvre les moyens nécessaires permettant d'assurer le respect des dispositions de confidentialité liées au projet et s'engage à respecter l'annexe II du CCAP « ERR » du présent accord-cadre.

VI.2 DOSSIER DE PILOTAGE, TABLEAUX DE BORD ET INDICATEURS

Le dossier de pilotage est un document de synthèse à destination de l'administration, établi et transmis par les titulaires avant chaque comité contractuel.

Le dossier de pilotage est constitué de tableaux de bord regroupant les indicateurs et les éléments d'accompagnements nécessaires à leur exploitation (définition des indicateurs, explication, mode d'obtention ou de calculs, explication des valeurs anormales, etc.).

Le dossier de pilotage apporte une visibilité claire sur les thématiques suivantes :

- l'activité et la qualité de la réalisation ;
- les risques (techniques, calendaires, budgétaires, etc.) ;
- les décisions prises en comité ;
- éventuellement, les budgets (prévisionnel, état de la consommation, état de la facturation).

Concernant les indicateurs contractuels de qualité d'activité et de réalisation, la liste non exhaustive dressée ci-dessous constitue le minimum requis :

- respect des délais et des critères de réception contractuels ;
- conformité et disponibilité de la totalité des résultats et des livrables attendus ;
- maîtrise des délais (prise en compte, réponse aux demandes de service) ;
- garanties de bonnes conditions d'exécution du marché (transparence des résultats de pilotage, qualité et stabilité des équipes, conformité des processus) ;
- synthèse sur la répartition des demandes ;
- calendrier des actions à venir en rapport aux prochaines livraisons ;
- état d'avancement ou bilan des livraisons effectuées ;
- état des lieux de la production documentaire ;
- ressources humaines mises en place.

VI.3 HORAIRES D'EXECUTION

La totalité des prestations du marché s'exécute en jours ouvrés de l'administration, en heures ouvrées (HO), de 08h00 à 18h00.

De façon exceptionnelle, les prestations peuvent également s'exécuter :

- en semaine, en heures non ouvrées (HNO), de 18h00 à 08h00 ;
- le week-end (du vendredi 18h00 au lundi 08h00) ;
- les jours fériés.

VII. LOT 1 : CONCEPTION, DEVELOPPEMENT ET MAINTENANCE DES BRIQUES LOGICIELLES DU CBIMI

VII.1 PRESENTATION DU LOT 1

Ce lot concerne la conception, l'intégration des briques éditeurs et le développement logiciel nécessaire à la construction du CBIMI dont le périmètre est évoqué à l'article II du présent CCTP.

Dans le cadre de cette phase de développement, le titulaire du lot 1 s'appuie sur les logiciels fournis par les lots 2 et 3, qui constituent des éléments essentiels pour la mise en œuvre des fonctionnalités requises. L'ensemble de ces « briques » techniques constitue la base pour la construction du CBIMI.

Cette prestation inclut également des missions d'expertises, visant à accompagner la mise en œuvre du CBIMI dans son intégralité.

Ce lot est composé de 4 prestations :

LOT 1	Conception, développement et maintenance des briques logicielles du CBIMI
Prestation L1P1	Initialisation de l'accord cadre et prise de connaissance du CBIMI et reprise du composant de captation
Prestation L1P2	Étude de faisabilité
Prestation L1P3	Réalisation et maintenance du CBIMI en mode Agile
Prestation L1P4	Réversibilité

VII.2 ÉQUIPE DU TITULAIRE

Pour réaliser les prestations du Lot 1, l'équipe du titulaire présente les profils et niveaux de séniorité suivants (le titulaire pourra proposer des profils complémentaires s'ils s'avèrent nécessaires à la réalisation des prestations) :

L'expertise Delivery Manager doit inclure les activités de pilotage contractuel.

Les fonctions Proxy PO et Scrum Master seront bien couvertes par les UO " PO Proxy" et "Scrum master". L'administration estime qu'un PPO peut intervenir sur 1 à 2 features teams, idem pour le Scrum Master. Cependant le candidat est invité à détailler son organisation type pour garantir la performance de ses équipes et le respect de la méthode de Delivery retenue. Ce faisant le candidat est libre de proposer toute optimisation possible.

Pour les prestations de développement, le titulaire doit s'assurer de la prédictibilité de son équipe et s'assurer que le ratio « vitesse mesurée/vitesse moyenne (ou planifiée) » soit supérieure à 80%.

Lot 1	Séniorité exigée ¹
Delivery manager	J,C, S
Chef de projet	J,C, S
Tech Lead	J, C, S,E

1 J : Junior, C : Confirmé, S : Sénior, E: Expert

PO Proxy	J, C, S
Développeur full stack	J, C, S
Développeur back	J, C, S
Développeur front	J, C, S
Consultant technique	J, C, S, E
Urbaniste	J, C, S
Architecte SI	J, C, S
Architecte logiciel	J, C, S
Architecte Safe	J, C, S, E
Scrum Master	J, C, S
OPS / Devops / DevSecOps	J, C, S, E
UX /UI designer	J, C, S, E
Data scientist	C, S, E
Data Architect / Data Engineer	C, S, E
Consultant IA	J, C, S, E
Expert SSI	C, S
RTE (Release Train Engineering)	C, S, E
Coach Agile à grande échelle	C, S
CO-PO ou PO Proxy	J, C, S, E
Autre Expertise (RGPD (Règlement Général sur la protection des données), base de données, etc.)	J, C, S, E

Le ministère autorise l'ajout de profils.

VII.3 PRESENTATION DE LA DEMARCHE AGILE POUR LE LOT 1

VII.4 L'EQUIPE MULTIDISCIPLINAIRE ET LA VISION PRODUIT

Le développement et la maintenance s'organisent autour de la ligne des produits Biométriques

Un ou plusieurs Business Owners (au sens de la méthode SAFe) de la MOA sont responsables de chaque ligne de produit. Au sein des lignes de produit, les équipes se répartissent en « feature team » ou « component team ». Il s'agit d'équipes multidisciplinaires intégrées (Dev et Ops) responsables de toute la chaîne de réalisation d'une fonctionnalité ou d'un composant technique, parfaitement autonomes et délivrant de la valeur de bout-en-bout.

Toutes les équipes poursuivent un objectif commun de qualité et d'excellence globale dans la production de valeur en continu afin de maintenir et faire évoluer le CBIMI et son intégration dans les applications biométriques métier. Il appartient au titulaire de diffuser auprès de ses équipes des pratiques de bonne

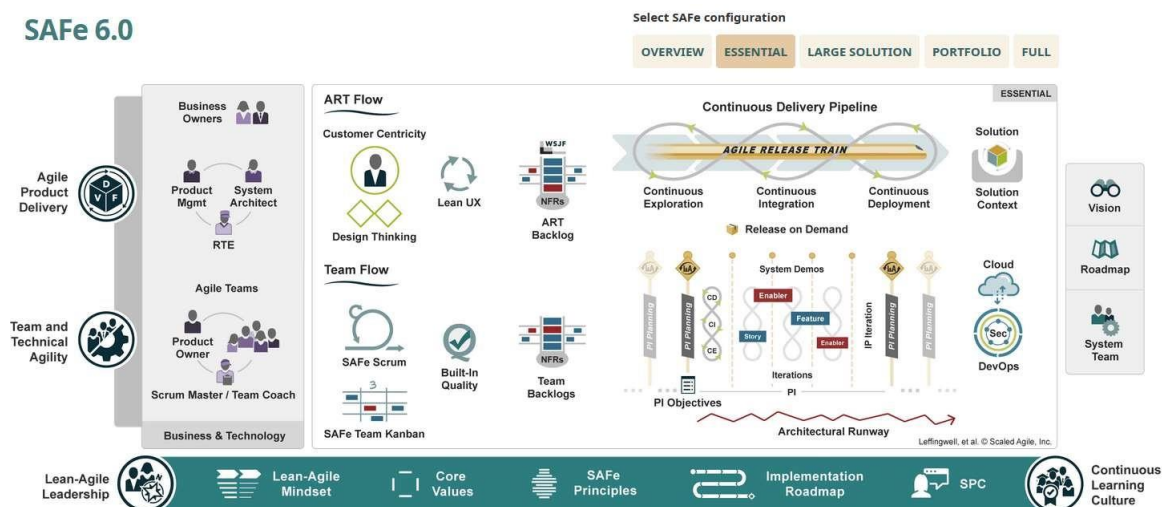
collaboration et d'entraide avec les intervenants de l'administration et des éventuels autres fournisseurs, et de garantir le respect des rôles et des responsabilités de chacun.

En amont, l'administration procédera à un cadrage et un lancement de projet qui fixera les rôles de chaque acteur.

VII.5 L'AGILITE A GRANDE ECHELLE

Les processus utilisés sont issus des méthodes Scrum, Kanban, XP et SAFe et respectent les éléments clés suivants :

La mise en place de **SAFe 6.0** a minima dans version « Essential »



L'administration et le titulaire s'attachent à renforcer la maîtrise du SI cible par les agents de l'administration. Ces derniers assurent les fonctions suivantes :

- la direction de programme est assurée par la MOA (section produit migratoire et biométrie applicative du bureau BADM de la SDAN pour le CBIMI), la MINUM et les directions métiers ou directions d'applications;
- la direction technique est assurée par la DTNUM (MOE) ;
- la gestion de produit (Business Owners et Product Managers) est assurée par la MOA. La mission de Product Owner est assurée en priorité par la MOA et fera l'objet d'un renfort par une AMOA à la demande de l'administration si utile;
- les fonctions de Proxy Product Owner (ou CO-PO), de tech lead et de scrum master sont assurés par le titulaire et font partie de la « feature team » ;
- l'ingénierie du « Train SAFe » (Release Train Engineer ou RTE) est assurée par le titulaire du lot 1 et doit faire l'objet d'une concertation régulière avec la MOA;
- l'architecture SI et solution est proposée par le titulaire et validée par la DTNUM en accord avec la MOA ;
- l'exploitation, l'intégration et le DevSecOps sont assurés par le titulaire avec l'appui et la validation de la DTNUM ;
- un backlog établit la liste des fonctionnalités métier ou technique, découpées en epics / features / user stories ;
- la priorisation du backlog est aux mains des représentants du produit (BO, PO, chef de produit) ;
- le temps de développement est divisé en incréments. Un incrément est composé de cinq (5) itérations de deux (2) semaines. Des rituels de PI Planning et d'Inspect & Adapt sont organisés à la fin de chaque incrément pendant la cinquième itération ;

- une démonstration et une rétrospective sont organisées à la fin de chaque itération ;
- un management visuel est utilisé et valorisé ;
- le workflow général est affiché sur un tableau (appelé « kanban ») établi en étapes / colonnes (exemple : à cadrer, à développer, en cours, à recetter). Les colonnes peuvent évoluer ;
- l'état d'avancement des user stories (fonctionnelles, techniques ou bugs) est indiqué sur le kanban. Le nombre d'items qui peuvent être placés dans chaque étape du workflow est limité ;
- le tableau est visualisable sous format papier (brown paper) et numériquement (exemple : JIRA). Toute l'équipe doit pouvoir le visualiser ;
- dans la pratique, l'équipe de développement est organisée afin de maximiser sa productivité, garantir un produit robuste, renforcer la propriété collective du code et s'auto-améliorer en continu. Pour ce faire les actions suivantes sont prévues :
 - mise en place des tests automatiques pour toutes les fonctionnalités ;
 - une collaboration entre développeurs (pair programming, mob programming, dojo, revue de code,.) ;
 - des formations collectives ;
 - utilisation du refactoring ;

Cette méthode pourra être adaptée dans ses éléments clés (configuration et composition de l'équipe, déroulement des itérations, durée des itérations et durée des incréments, etc.) en fonction des sujets abordés.

VII.6 L'AGILITE A PETITE ET MOYENNE ECHELLE

Quand les caractéristiques du composant à développer ou de ses évolutions ne justifient pas la mise en place d'une organisation agile à grande échelle (taille de l'équipe, absence de liens entre les produits, grande hétérogénéité technique, etc.), les équipes s'organisent en Agile selon les méthodes Scrum, XP et Kanban, et respectent les éléments clés suivants :

- L'administration et le titulaire s'attachent à renforcer la maîtrise du SI cible par les agents de l'administration. Ces derniers assurent les fonctions suivantes :
 - la direction de programme est assurée par la MOA ;
 - la direction technique est assurée par la DTNUM (MOE) ;
 - la gestion de produit (Business Owners et Product Managers) est assurée par la MOA avec l'appui de l'AMOA. La mission de Product Owner est assurée en priorité par la MOA et fera l'objet d'un renfort par l'AMOA à la demande de l'administration ;
 - les fonctions de Proxy Product Owner (ou CO-PO), de tech lead et de scrum master sont assurés par le titulaire et font partie de la feature team ;
 - l'architecture SI et solution est proposée par le titulaire et validée par la DTNUM en accord avec la MOA ;
 - l'exploitation, l'intégration et le DevSecOps sont assurés par le titulaire avec l'appui et la validation de la DTNUM ;
- un backlog établit la liste des fonctionnalités métier ou technique, découpées en epics / features ou Enablers /user stories ;
- la priorisation du backlog est aux mains des représentants du produit (BO, PO, chef de produit) ;
- le temps de développement est divisé en incréments. Un incrément est composé de cinq (5) itérations de deux (2) semaines. Des rituels de PI Planning et d'Inspect & Adapt allégés sont organisés à la fin de chaque incrément pendant la cinquième itération ;
- une démonstration et une rétrospective sont organisées à la fin de chaque itération ;
- un management visuel est utilisé et valorisé ;
- le workflow général est affiché sur un tableau (appelé « kanban ») établi en étapes / colonnes (exemple : à cadrer, à développer, en cours, à recetter). Les colonnes peuvent évoluer ;
- l'état d'avancement des user stories (fonctionnelles, techniques ou bugs) est indiqué sur le kanban. Le nombre d'items qui peuvent être placés dans chaque étape du workflow est limité ;
- le tableau est visualisable sous format papier (brown paper) et numériquement (exemple : JIRA). Toute l'équipe doit pouvoir le visualiser ;
- dans la pratique, l'équipe de développement est organisée afin de maximiser sa productivité, garantir un produit robuste, renforcer la propriété collective du code et s'auto-améliorer en continu. Pour ce faire les actions suivantes sont prévues :

- mise en place des tests automatiques pour toutes les fonctionnalités ;
- une collaboration entre développeurs (pair programming, mob programming, dojo, revue de code, etc.) ;
- des formations collectives ;
- utilisation du refactoring ;
- etc.
- Cette méthode pourra être adaptée dans ses éléments clés (configuration et composition de l'équipe, déroulement des itérations, durée des itérations et durée des incréments, etc.) en fonction des sujets abordés.

VII.7 L'EXCELLENCE TECHNIQUE

Les développements suivent les pratiques XP (eXtreme Programming) :

- intégration et déploiement continue en s'appuyant sur les outils de la DTNUM et en les complétant si nécessaire ;
- une pratique rigoureuse de la qualité logicielle en appliquant le Test Driven Development, la revue de code, le Clean Code et la conception simple ;
- la culture des tests automatisés dès l'expression du besoin en s'appuyant notamment sur le Behavior Driven Development. L'évolution du nombre de tests automatiques est un indicateur de qualité suivi par l'équipe.

VII.8 UNE APPROCHE UX EN CONTINU

L'expérience utilisateur doit être au cœur de la démarche de conception et de réalisation des produits. Le produit ainsi construit est utile, ergonomique et accessible à tous.

VII.9 OPTIMISATION DU TIME TO CITIZEN ET DU TIME TO REPAIR

Le titulaire s'attache à optimiser le « Time To Citizen » ou TTC (temps nécessaire à la mise en service effective d'une nouvelle fonctionnalité, équivalent du Time To Market dans le domaine privé) et le « Time To Repair » ou TTR (temps nécessaire à la mise en service effective d'une correction). Ce temps est calculé sur l'ensemble de la chaîne, de la conception à la mise en production effective sans régression. Pour ce faire le titulaire exploite les optimisations offertes par l'infrastructure (Cloud MI, Cloud externe, ISOCELE) et applique une méthode DevSecOps rigoureuse qui consiste à :

- concevoir des architectures et des patterns cloud natives répondant aux préoccupations des Dev et des Ops ;
- construire et maintenir l'infrastructure par du code en utilisant des outils d'automatisation adéquats ;
- mettre en œuvre des outils et des processus de construction et de déploiement continus en s'appuyant et en complétant les outils de la DTNUM ;
- s'assurer de la diffusion d'une culture DevSecOps au sein de ses équipes ;
- former l'ensemble de ses intervenants au DevSecOps ;
- favoriser un dialogue constant entre Dev et Ops.

VII.10 DEMARCHE DE TESTS, D'INTEGRATION ET DE DEPLOIEMENT EN CONTINU

Le titulaire est responsable de l'exécution de tests automatisés, de l'intégration et du déploiement en continu des développements réalisés au titre du présent accord-cadre. La démarche d'intégration et de déploiement en continu permet de générer des builds (compilations), de les vérifier (ensemble des vérifications garantissant le respect des critères d'acceptation et des exigences) et de les déployer de manière automatisée sur l'infrastructure « cloud » de l'administration. Cette démarche permet, entre autres, de :

- vérifier le bon fonctionnement technico-fonctionnel du produit global ;
- vérifier la non-régression des fonctionnalités déjà développées ;
- détecter d'éventuels problèmes d'intégration au plus tôt lors du développement.

Au cours des itérations, le titulaire livre de manière continue les fonctionnalités développées par ses équipes, et l'administration vérifie le bon fonctionnement fonctionnel et technique de celles-ci, à partir des « user stories », du « product backlog » actualisé et de la démonstration du résultat de l'itération par le titulaire.

Les tests automatisés des développements doivent inclure, a minima, les tests suivants :

- tests de bon fonctionnement de bout en bout au niveau fonctionnel (conformité avec les critères d'acceptation des user stories) ;
- tests de bon fonctionnement de bout en bout au niveau technique (absence de génération d'erreur ou d'exception) ;
- tests de qualité du code ;
- tests de sécurité statiques et dynamiques ;
- tests de non-régression fonctionnelle et technique ;
- tests de performance ;
- tests de charge ;
- tests de résilience ;
- tests d'intégration technique.

VII.11 DEFINITION DE TERMINE OU « DEFINITION OF DONE » OU « DoD »

Une fonctionnalité est réputée terminée et pouvant être réceptionnée par l'administration quand elle remplit l'ensemble des conditions suivantes :

- Les standards de code et les décisions d'architecture sont respectés ;
- Les exigences non fonctionnelles sont respectées (accessibilité, sécurité, performance, etc.) ;
- La merge request (MR) porte la référence du ticket Jira ;
- Le bon niveau de test est appliqué : types de tests, couverture, nombre de tests appropriés ;
- L'ensemble des tests bout-en-bout, de non régression, fonctionnels, d'intégration et unitaires sont passants ;
- La documentation métier comme technique est mise à jour ;
- Une revue de code a été effectuée par un relecteur différent du développeur ;
- Tous les retours de code review ont été pris en compte et le ticket a été mergé sur master ;
- Les étapes de la pipeline d'intégration et de déploiement continus sont passantes ;
- Tous les critères d'acceptation ont été validés sur un environnement iso-production ;
- Le ticket a été livré en production (La fonctionnalité correspondante à ce ticket peut avoir été ou non mise en service, la mise en service pouvant être décorrélée de la mise en production) ;
- Le Product Owner a validé que l'élément répond aux critères d'acceptation et satisfait les besoins métier.

VII.12 GOUVERNANCE DE LA DEMARCHE AGILE ET DISPONIBILITE DES INTERVENANTS

VII.13 RITUELS EQUIPE

Les rituels organisés au niveau d'une équipe ont pour objectifs de :

- se synchroniser dans l'équipe ;
- cadrer et approfondir le « backlog » ;
- favoriser l'amélioration continue et la montée en compétence ;
- montrer l'avancement.

Les rituels concernés sont les suivants :

- **rituels agile "classiques" :**
 - « daily stand up » ;
 - « poker planning » ;
 - « backlog grooming » ;
 - revue d'itération ;
 - rétrospective ;
 - démonstration d'équipe ;

- **rituels techniques :**
 - rétrospective technique ;
 - revue de code à deux ou en équipe.

Le temps consacré à ces rituels est considéré comme du temps de développement.

VII.14 DISPONIBILITE DES INTERVENANTS ET STABILITE DE L'EQUIPE

Une équipe produit « feature team » / « Component team » doit être stable et les changements d'acteurs doivent être limités et sans impact sur la feuille de route du produit ainsi :

- le titulaire s'assure de la disponibilité des intervenants pendant la durée du développement d'une « feature » ou d'un « enabler » (un incrément de programme). A l'exception d'un cas de force majeure, il n'est pas accepté de remplacement d'intervenant pendant le développement d'une « feature » ou d'un « enabler » ;
- entre deux incréments de programme (dix semaines), le titulaire peut proposer le remplacement d'un intervenant, le taux de rotation ou « turn-over » ne peut dépasser 4 % de l'ensemble des effectifs entre deux incréments ;
- en cas d'insuffisance d'un intervenant, l'administration peut demander au titulaire son remplacement dans les conditions fixées à l'exigence ERT11 exposée à l'article V.5. ;
- Chaque remplacement doit être organisé de manière à limiter l'impact sur la feuille de route du produit. Le titulaire doit s'assurer d'un recouvrement pendant au moins deux itérations entre l'intervenant sortant et l'intervenant entrant.
- Les recouvrements ne donnent lieu à aucune facturation supplémentaire (seul un profil sur les deux est facturé).

Le titulaire doit disposer de ressources suffisantes pour couvrir l'ensemble des prestations de son lot.

Les profils experts doivent justifier d'une formation et d'une expérience significative dans leur domaine d'expertise. Tous les intervenants doivent justifier à minima d'une première formation ou d'une première expérience dans l'agilité. Le titulaire est responsable du plan de développement des compétences de leurs équipes de manière à maintenir un fort niveau d'excellence et une forte motivation.

VII.15 VELOCITE

La vélocité est un indicateur important pour le fonctionnement de l'équipe, elle permet notamment de lever les incertitudes sur les développements à venir.

Chaque « user story » reçoit une estimation. Elle est exprimée en point initial de complexité (« story point ») avant son développement. L'équipe s'engage, au début de chaque itération, en fonction de la taille de l'équipe (absence, congés, etc.), du temps imparti (jours fériés, réunions, etc.) et en se basant sur l'historique des itérations passées, sur un nombre de points de complexité à réaliser. Seules les « stories » effectivement réalisées (« done ») rentrent en compte dans le calcul du nombre de points effectués dans une itération donnée. Ce nombre de points effectivement réalisés est appelé « vélocité ». Cet indicateur peut varier d'une itération à l'autre.

Il est toutefois fiabilisé par une moyenne constituée au fil des itérations passées (au sein d'une équipe, elle est stabilisée en moyenne à partir de la troisième itération).

Après la période de stabilisation (typiquement trois itérations), la variation de la vélocité ne doit pas dépasser 20% de la moyenne calculée sinon une itération permettant d'absorber le surplus est ajouté, à la charge du titulaire

La proportion réservée à la correction des anomalies pour une itération ne peut excéder 20%. Au-delà, une itération supplémentaire à la charge du titulaire est mis en œuvre pour résorber le surplus d'anomalies

Toute baisse importante de la capacité à faire de l'équipe dépassant 20% (liée par exemple à des absences prolongées, congés, etc.) doit être signalée à l'administration avant le PI Planning de la ligne de produits concernée. Dans la mesure où cette baisse impacte le nombre de fonctionnalités pouvant être produites par le titulaire sur l'incrément, cette baisse est répercutée dans le bon de commande de l'incrément concerné conformément à la formule d'évaluation des coûts.

Cette vélocité est calibrée d'un commun accord entre la MOA et le titulaire en fonction de la composition des équipes lors des premières itérations et en tenant compte :

- De la quote-part allouée à la correction des anomalies et à la réduction de la dette technique et sécuritaire (20%) ;
- De la quote-part allouée aux cérémonies agiles (7%) ;

VII.16 METHODE D'ESTIMATION DE L'EFFORT

L'estimation de l'effort demandé par une story (qu'elle soit fonctionnelle ou technique) se base sur trois critères :

- La difficulté intellectuelle à réaliser la Story. Exemple : trouver l'algorithme de calcul qui convient.
- La lourdeur, c'est-à-dire le travail, probablement répétitif ou long, qui est nécessaire pour réaliser la Story/ l'enabler. Exemple : changer le nom des classes dans tout le code, factoriser le libellé d'un champ visible sur toutes les pages de l'application, etc.
- L'incertitude, c'est-à-dire le manque d'information au moment de l'estimation pouvant rendre difficile l'estimation de la lourdeur ou de la complexité de la Story. Exemple : interfacier l'application à un système tiers sans avoir suffisamment d'informations sur les données à échanger.

Taille d'une Story :

- Petite : tous les critères sont de niveau bas,
- Moyenne : tous les critères sont de niveau bas ou moyen, avec au moins un niveau moyen,
- Grande : un critère est de niveau élevé,
- Très grande : plusieurs critères sont de niveau élevé.

Taille de Story	Description	Points de complexité
Petite	Tous les critères sont de niveau bas	2
Moyenne	Tous les critères sont de niveau bas ou moyen, avec au moins un niveau moyen	5
Grande	Un critère est de niveau élevé	8
Très grande	Plusieurs critères sont de niveau élevé	13

Chacun de ces trois critères est défini selon trois niveaux : bas, moyen ou élevé. Leur évaluation permet ensuite de distinguer quatre tailles de Story.

VII.17 ENGAGEMENTS LIES AU BON FONCTIONNEMENT

Le produit livré est considéré comme fonctionnel quand son bon fonctionnement est constaté sur l'environnement de production. Le titulaire doit s'adapter au contexte et exigences de l'administration de l'intérieur en termes d'hébergement, d'exploitation et de supervision. L'administration ne peut être tenue responsable des éventuels écarts de fonctionnement du produit entre l'environnement de production et ceux de développement et de test.

VII.18 MESURE DE LA PERFORMANCE (METRIQUES)

Les métriques de suivi de la qualité logicielle sont calculées et relevées à chaque incrément.

Les métriques prévues par le « Scaled Agile Framework » SAFe sont aussi relevées et suivies lors des comités et rituels de la ligne de produits ou des équipes.

Dans tous les cas de figure, le titulaire s'engage à respecter les métriques suivantes par incrément :

Engagement de qualité	Mesure	Seuils à respecter
Respect des compétences requises	Nombre de remplacements demandés par l'administration pour défaut de compétences	Pas plus de deux remplacements par incrément (trois (3) mois)
Respect de la stabilité de l'équipe.	Nombre de remplacements d'intervenants à l'initiative du titulaire	Aucun remplacement pendant un incrément. Taux de rotation inférieur à 4% entre deux incréments.
Respect du recouvrement de profil en cas de départ	Nombre de jours de recouvrement entre le profil sortant et le profil entrant	Au-moins deux itérations de recouvrement
Prédictibilité à l'échelle de l'équipe	Vélocité mesurée / Vélocité moyenne (ou planifiée)	Supérieure à 80%
Prédictibilité à l'échelle de la ligne de produits	Valeur métier (Business Value ou BV) réellement réalisée et validée / Valeur métier planifiée	Supérieure à 80%
Avancement des features et des enablers	Nombre de features et enablers validés (ayant atteint le DoD) / Nombre de features et enablers planifiées	Supérieur à 100%

VII.19 TAUX D'ÉCHEC DES CHANGEMENTS :

Le taux d'échec des changements (Change Failure Rate) doit être inférieur à 30% sur une période de 1 an glissant.

Le calcul du CFR sera effectué en utilisant la formule suivante : (nombre de MEP avec régression / nombre total de MEP) x 100.

Tout dépassement du taux d'échec maximal entraînera l'application de pénalités conformément au CCAP.

VII.20 PRESTATION L1P1 - INITIALISATION DE L'ACCORD CADRE, PRISE DE CONNAISSANCE DU CBIMI ET REPRISE DU COMPOSANT DE CAPTATION

OBJECTIFS DE LA PRESTATION

Cette prestation consiste en :

- la prise de connaissance des environnements organisationnel, fonctionnel et technique nécessaire à la conception et au développement du CBIMI ;
- la mise en place de l'organisation de travail du titulaire, des environnements de développement et de maintien en condition opérationnelle (MCO) de la solution cible, des outils associés et des dispositions en matière de qualité et de sécurité²;
- la mise en place de son organisation de pilotage des prestations et des outils de *reporting* auprès de l'administration ;
- la mobilisation et la montée en compétences des équipes du titulaire ;
- la reprise du composant de captation :
 - s'approprier le composant de captation : acquérir les connaissances fonctionnelles et techniques nécessaires ;
 - installer l'ensemble des composants techniques (codes sources...) dans son environnement de développement ;
 - prendre en charge de façon progressive les opérations de MCO ;
 - élaborer ou mettre à jour la documentation au composant de Captation.

Un transfert de responsabilité sera prévu entre les équipes en charge du développement du composant de captation vers le titulaire du présent lot. Ce transfert de responsabilité se matérialisera par un procès-verbal validant le fait que le titulaire dispose des éléments nécessaires à la réalisation des prestations avec le niveau de service requis.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation, le titulaire doit, au travers d'ateliers ou de travail en collaboration avec les équipes actuelles réaliser les tâches suivantes :

Pour l'initialisation de l'accord cadre et la prise de connaissance

Initialisation

- Organiser la réunion de lancement.
- Définir le Plan d'action précis de cette prestation d'initialisation (étapes, tâches, méthodologie, livrables, intervenants du titulaire, planning d'initialisation).
- Conduire les réunions d'initialisation.

Rédaction des documents relatifs à l'initialisation du marché

- Élaborer le Plan d'Assurance (PAQ) ;
- Rédiger le Plan d'Assurance Sécurité (PAS) et la continuité de reprise d'activité (PCA/PRA) pour assurer la continuité de ses activités en cas de sinistre sur les moyens du titulaire dédiées à la réalisation du présent accord-cadre ;

² L'administration pourra demander de procéder à un audit des environnements mis en place par le titulaire.

- Définir les modalités de pilotage et de suivi - Proposer et produire les modèles de support et de tableau de bord de suivi des prestations et en accord incluant la mise en œuvre des indicateurs ;
- Prendre connaissance des composants des titulaires des lots deux (2) et trois (3) ;
- Construire la chaîne de Delivery avec les environnements à mettre en place par le titulaire ;
- Produire un kit d'accueil nouvel arrivant.

Constitution de l'équipe cible :

- Transmettre les CV de chaque membre de l'équipe du titulaire pour réaliser les prestations (les CV ayant été préalablement contrôlés par le titulaire par rapport au fichier du casier judiciaire). Ce CV devra faire l'objet d'une validation de l'administration ;

Pour l'administration : lancer des enquêtes pour les prestataires (Le titulaire est susceptible de devoir fournir des éléments complémentaires : copies des CNI ou passeports).

Finalisation de l'initialisation de l'accord-cadre

- Une fois cette initialisation réalisée, le titulaire est responsable du maintien en interne des compétences de ses équipes. Les intervenants à suivre du titulaire doivent être préalablement informés du contexte grâce aux livrables de la phase d'initialisation, incluant notamment le kit d'accueil.

Pour la reprise du composant de captation :

La préparation :

- Analyser les éléments transmis
- Élaborer le plan de reprise du composant de captation (activités à réaliser, ateliers) et planning détaillé de prise de connaissance et définir les objectifs associés.
- Organiser les travaux et planifier les ateliers le cas échéant.

La mise en place du cadre de fonctionnement :

- Rédiger/ actualiser les documents techniques descriptifs ;
- Mettre en place son équipe.

La poursuite des travaux de réalisation, sous le contrôle de l'administration :

- S'approprier le « backlog » du composant de captation ;
- Sur demande de l'administration, participer à l'élaboration d'un panel de développements en collaboration avec l'administration et/ou le titulaire sortant.

Dresser un bilan démontrant la capacité du titulaire à réaliser seules prestations demandées.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration participe aux réunions permettant la compréhension des enjeux et fournit :

- Toute documentation utile pour la compréhension du périmètre du CBIMI (Note de cadrage, cas d'usages métier...) et notamment du composant de captation ;
- La description de l'environnement de développement nécessaire à la mise en place par le titulaire de sa plateforme ;
- Les processus de livraison des composants développés sur l'environnement d'intégration de l'administration ;
- Les PSSI applicables ;
- Une présentation de son organisation et des acteurs concernés (de l'administration).

L'administration cadre la coordination du titulaire avec les autres lots de l'accord cadre et d'autres acteurs externes nécessaires à la réalisation des travaux.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire sur la base d'un **prix forfaitaire** sur une durée de deux (2) mois.

Le prix de cette prestation est forfaitaire et inclut l'ensemble des tâches documentées ci-dessus. La prestation ne peut être commandée qu'une seule fois.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version validée par ses équipes.

VII.21 PRESTATION L1P2 - ÉTUDE DE FAISABILITE

OBJECTIFS DE LA PRESTATION

Cette prestation consiste en la production d'études de faisabilité fonctionnelle et/ou technique afin de soutenir les choix et arbitrages concernant le CBIMI (définition et modifications de périmètre, identification de solutions techniques, etc.).

Ce type d'étude permet d'affiner l'expression de nouveaux besoins et/ou d'étudier la complexité technique et/ou ergonomique pour les prendre en compte dans le cadre d'évolutions du CBIMI.

Plusieurs types d'études peuvent être demandés :

- études de faisabilité, en vue notamment, d'accompagner l'administration sur l'élaboration d'un produit minimum viable (PMV) et de la Story Map du CBIMI;
- analyse de modules applicatifs extérieurs à intégrer dans le périmètre ;
- études d'impact technique ;
- étude de sécurité ;
- étude d'impact sur l'exploitation ;
- études de choix d'outils pour le programme ;
- identification des macros fonctionnalités ;
- etc...

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Prise de connaissance et définition de la méthodologie

- Le titulaire prend connaissance de la demande d'étude de faisabilité de l'administration et fournit la méthodologie avec le nombre d'ateliers et le planning associé pour réaliser la prestation.

Réaliser l'étude :

- Selon la méthodologie validée précédemment.

Restituer

- Organiser une réunion pour présenter les éléments de pré études à l'administration.

PREREQUIS FOURNIS PAR L'ADMINISTRATION
L'administration réalise une présentation de l'objet de l'étude.
TYPE DE PRIX
<p>Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur les unités d'œuvres (UO) selon la table des profils proposée par le titulaire et rappelant obligatoirement les travaux à réaliser, l'équipe et les livrables figurant au présent CCTP et le calendrier de réalisation.</p> <p>Préalablement à toute intervention, le titulaire présentera à l'administration le profil et le CV de son intervenant pour validation.</p>
LIVRABLES
La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

VII.22 PRESTATION L1P3 - REALISATION ET MAINTENANCE DU CBIMI EN MODE AGILE

OBJECTIFS DE LA PRESTATION
<p>Cette prestation a pour but de préparer la réalisation avec la rédaction des features, story mapping et user stories de développer l'ensemble des modules nécessaires à la constitution du CBIMI en mode produit, et d'en assurer la maintenance et les évolutions.</p> <p>Elle s'inscrit dans la logique de la démarche agile telle qu'exposée à l'article 0.</p>
DEFINITION DES ACTIVITES ET DES TACHES A REALISER
<p><u>Co constitution du backlog en collaboration avec l'équipe du ministère et son AMOA.</u></p> <p>L'AMOA de l'équipe CBIMI de l'administration :</p> <ul style="list-style-type: none"> organise les ateliers recueil du besoin métier avec les PO CBIMI, le proxy PO de ce lot (lot1), l'UX et tout autre intervenant nécessaire au déroulement de l'atelier ; centralise le besoin métier exprimer en atelier dans un document fonctionnel général (processus, maquettes, contexte, objectif, règles de gestion par fonctionnalité...) destiné au métier pour validation, au proxy PO de ce lot (lot 1) pour déclinaison en features et user stories et création du story mapping, aux recetteurs pour validation des livraisons; participe avec les équipes de ce lot (lot 1) du marché CBIMI et le PO CBIMI à la préparation et au déroulement des « pokers plannings » du fait de sa responsabilité sur la définition du « backlog » ; avec le PO CBIMI relit et valide les « user stories » rédigées par le proxy-PO du lot 1 ; complète les critères d'acceptation et les tests liés des « users stories » si besoin ; <p><u>Développement et maintenance évolutive :</u></p> <p>Au titre des activités de développement ou de réalisation des évolutions en mode agile, le titulaire doit :</p> <ul style="list-style-type: none"> définir avec le Product Owner les User Stories (US) de l'itération N+1 suivante ; rédiges les features et US des itérations suivantes, créer ou mettre à jour le story mapping ; planifier l'itération N avec le Product Owner (revue des stories, définition des critères d'acceptance, estimation en story points, validation du contenu de l'itération selon la vélocité

connue ou la capacité calculée). L'équipe doit inclure dans chaque itération des corrections de bugs et la réduction de la dette technique et sécuritaire ;

- développer et tester les stories ainsi définie de l'itération N selon l'approche agile retenue ;
- procéder à la livraison en état de fonctionnement du contenu de l'itération sur les environnements de test et de pré-production ;
- procéder en fin d'itération à la démonstration du système (System Demo au sens SAFe) intégrant tous les composants et features développés par toutes les équipes ;
- procéder à la rétrospective de l'itération. ;
- mettre à jour la documentation du produit (DAT, dossier fonctionnel, dossier d'exploitation, guide utilisateur, wiki) ;
- à la demande de l'administration, procéder avec l'aide des OPS (du titulaire et de la DTNUM) à la mise en production / mise en service du produit (Release On Demand) ;
- participer à la préparation des rituels du programme notamment en fin d'incrément (System Demo, Inspect and Adapt, PI Planning) ;
- suivre la vélocité de l'équipe et les indicateurs du marchés, préparer un reporting pour l'administration lors des comités projet
- en cas de changement de l'équipe en charge du développement et de la maintenance d'un composant, soit pendant son développement soit après sa mise en service, assurer le transfert de compétences à destination de la nouvelle équipe.

La cinquième itération de chaque incrément est consacrée à l'innovation et à la planification conformément à la méthodologie SAFe.

D'une durée de deux semaines, cette itération est consacrée:

- à finaliser les développements pour atteindre les objectifs de l'incrément ;
- à la dernière démonstration du système de l'incrément ;
- au rituel Inspect and Adapt ;
- à la préparation et à l'exécution du rituel de PI Planning ;
- à l'affinage du Backlog et à la finalisation de la priorisation ;
- à l'intégration et aux tests finaux du produit obtenu à la fin de l'incrément ;
- à l'innovation et à l'exploration à l'initiative des équipes ou du programme (l'intention devant être utile aux produits, le temps alloué est validé par l'administration) ;

Au titre de la maintenance en conditions de sécurité (MCS), le titulaire doit :

- Analyser les bulletins d'alerte des composants et applications du périmètre du lot ;
- Analyser & identifier les impacts des correctifs de sécurité ;
- Concernant les alertes à prendre en compte, appliquer les recommandations ;
- Le titulaire adresse mensuellement à l'administration un bilan des alertes, avis et recommandations effectuées sur la période écoulée avec pour chacune d'elles :
 - Le n° d'identification des tickets de l'administration
 - La préconisation ;
 - Le descriptif de la préconisation
 - La tenue de ces objectifs est évaluée au travers de l'examen, en Comité de sécurité (article III.4 « comité de sécurité »), d'indicateurs décrits dans le Plan d'Assurance Sécurité.
- Accompanyer l'administration et se mobiliser dans le cadre d'une campagne de bug bounty lorsque demandé par l'administration.

Traitement des anomalies :

Le titulaire doit inclure dans chaque itération des corrections de bugs et la réduction **de la dette technique ou sécuritaire**.

On distingue les niveaux d'anomalies suivants :

- **anomalie bloquante** : bloque le fonctionnement du produit. Tout incident produisant l'altération de données ou qui interdit l'accès normal aux données (en lecture et/ou en écriture), ou qui rend impossible l'utilisation normale d'une fonction, de façon réhibitoire et

non contournable par l'administration sans intervention du titulaire. Est reproductible et le processus de reproduction peut être décrit ;

- **anomalie majeure** : interdisant la mise en œuvre d'une ou plusieurs fonctionnalités du produit, sans qu'il existe de solution de contournement acceptable par les utilisateurs en termes de coût et d'organisation. Est reproductible et le processus de reproduction peut être décrit ;
- **anomalie mineure** : anomalie portant sur une ou plusieurs fonctionnalités, n'empêchant pas leur fonctionnement et ne produisant pas d'altération de données ou des résultats, mais rendant l'usage des fonctionnalités plus compliquée et l'augmentation des temps de traitement. Ce type d'anomalie implique soit la correction de l'anomalie soit la mise en œuvre d'un moyen de contournement pouvant être mis en œuvre par un utilisateur pour parvenir au résultat attendu.

En cas de désaccord sur la qualification de l'anomalie entre l'administration et le titulaire, le niveau de gravité qui est retenu est celui proposé par l'administration.

En phase de développement, la part de cette activité corrective ne dépasse pas en story points 20% du contenu de l'itération. Si la part de correction des anomalies d'une itération courante est inférieure à 20% du contenu de l'itération suivante, la correction des anomalies mineures de l'itération courante est effectuée dans l'itération suivante et ne donne pas lieu à une contrepartie financière.

Les délais de correction des anomalies sont mentionnés dans le tableau ci-après et courent à partir de la remontée de l'incident par l'administration ou par le Product Owner et ce par tout canal approprié (téléphone, mail ou via les fiches « incidents » sur l'outil de suivi des incidents, retenu par l'administration dans le cadre de la prestation 1 d'initialisation du programme). La correction est soit définitive, soit une solution de contournement est mise en place par le titulaire pour pallier le dysfonctionnement. Les jours ouvrés sont tous les jours du lundi au vendredi compris, à l'exception des jours fériés légaux.

Les heures ouvrées sont fixées sur les tranches horaires suivantes : de 9h00 à 18h00.

	Anomalie bloquante	Anomalie majeure	Anomalie mineure
Délai de correction	1 jour ouvré	2 jours ouvrés	Au cours de l'itération suivante

La correction des anomalies bloquantes et majeures se fait, sans contrepartie financière, dans les délais indiqués dans le tableau ci-dessus sauf exception consentie par l'administration.

Lorsque le nombre d'anomalies (bloquante, majeure ou mineure) devient trop important pour être géré de la façon décrite ci-dessus ou si le nombre d'anomalies continue de croître, le titulaire propose à l'administration un plan de résorption des anomalies et assure une itération « réduite », dédiée à la correction d'anomalies, sans contrepartie financière de la part de l'administration.

Après la mise en service du composant développé :

Les anomalies détectées en production sont corrigées dans les délais indiqués dans le tableau ci-dessus. Le ratio entre correction d'anomalies, réduction de dette et développement de nouvelles fonctionnalités est décidé conjointement avec le Product Owner et l'administration en fonction, des besoins évolutifs identifiés et priorisés, du nombre d'anomalies identifiées et de leur niveau de sévérité et de la taille de l'équipe et de sa vitesse constatée (ou théorique à défaut).

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration :

- Fixe les objectifs et les priorités de chaque incrément de production au moyen d'un plan de release global et d'un backlog de fonctionnalités métier (Feature) et d'Enablers techniques priorisés à chaque incrément.
- Valide les livrables.
- Se prononce sur l'atteinte des objectifs de l'incrément.

Concernant le maintien en condition de sécurité, l'administration peut fournir les alertes ou impacts à analyser ponctuellement quand bien même l'identification des éléments est à la charge du titulaire de marché au titre de la prestation.

L'administration peut demander un accompagnement et une mobilisation du titulaire dans le cadre d'une campagne de « bug bounty ».

L'administration décide du cadre méthodologique à appliquer pour les développements après concertation avec le titulaire.

Ce cadre s'appuiera sur le framework SAFe pour l'agilité à grande échelle et sur la méthode Scrum et Kanban pour l'agilité au niveau de l'équipe. Des adaptations pourront être apportées à la méthode sur toute la durée de l'accord-cadre dans une logique d'amélioration continue.

TYPE DE PRIX

Chaque itération est définie par la combinaison d'une expertise de développement comme mentionnée ci-dessous et dans l'annexe financière avec si nécessaire une ou plusieurs autres expertises additionnelles :

- Expertise Delivery management ;
- Expertise Release train engineering ;
- Expertise Architecture SAFe ;
- Expertise Architecture SI ;
- Expertise CO-PO ou PO Proxy ;
- Expertise OPS / DevSecOps;
- Expertise Design UI ;
- ExpertiseDesign UX ;
- Expertise Scrum master ;
- Expertise CoachingAgilité à grande échelle ;
- Expertise Data science ;
- Expertise Data architect
- Expertise Data engineer;
- Expertise Expert SSI
- Expertise Expertise autre (RGPD, BDD, etc.).

On distingue quatre (4) niveaux de complexité pour les **Itérations** telles que définies dans l'annexe financière :

- Minimal (**M**) ;
- simple (**S**) ;
- moyen (M) ;
- complexe (**C**).

On distingue trois (3) niveaux de complexité pour les **expertises additionnelles** associées à des niveaux de séniorité telles que définies dans l'annexe financière :

- simple (**S**) ;
- moyen (**M**) ;
- complexe (**C**).

Domaine	Niveau de complexité	Charge estimée (j/h)
Développement d'une itération de deux (2) semaines soit 10 jours ouvrés.	Minimal	Une (1) itération nécessite la mobilisation d'un (1) développeur/ Tech Lead expérimenté à mi-temps + d'un (1) développeur full stack confirmé pendant deux semaines
Développement d'une itération de deux (2) semaines soit 10 jours ouvrés.	Simple	Une (1) itération nécessite la mobilisation d'un (1) développeur/ Tech Lead sénior + deux (2) développeurs confirmés pendant deux semaines
Développement d'une itération de deux (2) semaines soit 10 jours ouvrés.	Moyen	Une (1) itération nécessite la mobilisation d'un (1) développeur/ Tech Lead sénior + deux (2) développeurs confirmés + deux (2) développeurs juniors pendant deux (2) Semaines
Développement d'une itération de deux (2) semaines soit 10 jours ouvrés.	Complexe	Une (1) itération nécessite la mobilisation de deux (2) développeurs/ Tech Lead séniors + trois (3) développeurs confirmés + trois (3) développeurs juniors pendant deux (2) semaines
Expertise CO-PO ou PO Proxy	Simple	1
	Moyen	10
	Complexe	50
Expertise OPS / Devops	Simple	1
	Moyen	10
	Complexe	50
Expertise UI	Simple	1
	Moyen	10
	Complexe	50
Expertise Scrum Master	Simple	1
	Moyen	10
	Complexe	50
Expertise UX	Simple	1
	Moyen	10
	Complexe	50
Expertise Architecte SI	Simple	1
	Moyen	10
	Complexe	50
Autre Expertise (RGPD (règlement général sur la protection des données), base de données, etc.)	Simple	1
	Moyen	10
	Complexe	50
Coaching Agilité à grande échelle	Simple	1
	Moyen	10
	Complexe	50
Expertise Data Science	Simple	1

	Moyen	10
	Complexe	50
Expertise Data Architect / Data Engineer	Simple	1
	Moyen	10
	Complexe	50
Expertise SSI	Simple	1
	Moyen	10
	Complexe	50
Expertise : Release Train Engineering	Simple	1
	Moyen	10
	Complexe	50
Expertise Delivery management	Simple	1
	Moyen	10
	Complexe	50
Expertise Architecte système SAFe	Simple	1
	Moyen	10
	Complexe	50

Pour « Développement d'une itération de deux (2) semaines soit 10 jours ouvrés. » il convient d'intégrer dans la base tarifaire, les congés, les RTT et jours fériés non travaillés. Il conviendra que le candidat puisse expliciter sa proposition, l'abaque pris en compte sur ce sujet.

Les niveaux de séniorité des profils sont exposés à l'article V.5 (ERT3) du présent CCTP.

LIVRABLES

La liste des livrables est précisée ci-après et est rappelée également en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

Livrables	Délai de remise des livrables par le titulaire	Délais et modalités de vérification en jours ouvrés (*)
Code source relatif aux stories commandées, testé et documenté	A la fin de l'itération	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Rapport de la qualité du code (tests automatiques)	A la fin de l'itération	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Plan et résultats des tests de bon fonctionnement	A la fin de l'itération	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Documentation technique et fonctionnelle mise à jour (DAT, Dossier fonctionnel, dossier d'exploitation, dossier d'installation, guide	A la fin de l'incrément	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de

utilisateur, wiki)		l'incrément
Backlog de l'itération suivante affiné, priorisé, estimé (en story points), critères d'acceptation définis pour chaque user story	A la fin de l'itération	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de fin de l'incrément
Correctif ou la solution de contournement	Dans un délai d'un (1) ou deux (2) jours ouvré(s) ou à l'itération suivante (en fonction de la qualification de l'incident indiqué au -> traitement des anomalies) à compter de la signalisation de l'incident.	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Rapport d'expertise, si nécessaire	Dix (10) jours ouvrés à compter de la fin de l'expertise	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Bulletins d'alerte SSI hebdomadaire les lundis midi	Tous les lundis midi ouvrés ou le jour ouvré suivant dans le cas des lundis fériés.	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Bulletins d'alerte SSI urgents	Le jour de l'alerte dans le cas d'une alerte urgente	
Rapport d'analyse d'impact des correctifs de sécurité incluant les actions préconisées. Rapport des recommandations de correctifs de sécurité.	A la fin de l'itération	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Tableau de bord trimestriel de suivi SSI ; État mensuel des préconisations SSI	Au plus tard cinq (5) jours avant le comité de suivi sécurité pour le tableau de bord trimestriel. A la fin du mois pour l'état mensuel des préconisations SSI	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément
Rapport d'activité d'accompagnement des campagnes de Bug Bounty	Au plus tard dix (10) jours après la fin de la campagne.	Vérification définitive par l'administration dans un délai de vingt (20) jours ouvrés à compter de la fin de l'incrément

(*) La décision prise à l'issue des opérations de vérification est notifiée au titulaire par voie postale ou de messagerie électronique. Elle revêt la forme (au choix de l'administration) d'un message électronique simple ou d'un procès-verbal

L'objectif de réussite est attaché en priorité aux résultats et aux produits finaux, à la qualité et aux performances de ces produits et à la maîtrise des coûts de production.

Le titulaire s'engage à appliquer le cadre méthodologique général ci-avant défini, à favoriser et à suivre leur application par ses personnels et à procéder aux ajustements nécessaires quand une dérive ou une lacune est constatée (action de sensibilisation, formation complémentaire sans surcoût pour l'administration, remplacement, etc.).

VII.23 PRESTATION L1P4 – REVERSIBILITE

OBJECTIFS DE LA PRESTATION

L'objectif de cette prestation est de transférer l'ensemble des connaissances fonctionnelles et techniques sur l'ensemble du périmètre du lot, du titulaire vers l'administration.

Ce transfert peut être opéré vers la MOE, la MOA et/ou à tout tiers désigné par l'administration afin d'assurer une reprise rapide des prestations pour les produits du lot et sans désagrément pour les utilisateurs.

Assurer un transfert de tous les livrables informatiques, d'outillage, de documentations vers l'administration.

L'objectif de cette prestation est de permettre la reprise de l'ensemble des activités réalisées par le titulaire et par le personnel de l'administration.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Cette prestation peut être déclenchée par l'administration dans les trois cas suivants :

- en cas de résiliation du présent accord-cadre ;
- à la fin du présent accord-cadre ;
- en cas de reprise de la maintenance d'un produit du lot par les équipes de l'administration.

A l'issue du présent accord-cadre, le titulaire assure une totale réversibilité de l'ensemble des acquis relatifs aux prestations du présent lot. Le titulaire a l'obligation d'exécuter cette prestation et s'engage à apporter toute l'assistance nécessaire à la bonne fin de cette opération.

Pendant toute la durée de cette prestation, le titulaire reste pleinement responsable de ses engagements contractuels au titre de son obligation de résultat.

La prestation est assurée par des intervenants ayant participé / faisant partie de l'équipe du titulaire sortant.

Préparation

Le titulaire fournit la totalité de la documentation existante à jour ;

- propose un plan de réversibilité qui contiendra à minima un plan d'action détaillé incluant les prérequis ;
- une proposition d'organisation à mettre en place pour faciliter la transition entre l'ancien et le nouveau titulaire et le transfert de connaissances (ateliers Planning, etc...)
- transfère à l'administration les éléments suivants :
 - L'ensemble des logiciels et codes sources des composants applicatifs développés, les jeux de données utilisés pour les tests, le plan et les résultats des tests de bon fonctionnement ;
 - L'ensemble des documentations relatives aux composants applicatifs développés, incluant les spécifications fonctionnelles et techniques, le DAT, le dossier d'exploitabilité, les guides utilisateur, etc. ;
 - Les configurations de la solution mises en œuvre sur chaque application
 - L'ensemble des outils utilisés pour assurer la réalisation des développements, notamment les

outils liés :

- Au partage de documents ;
- Au suivi des développements ;
- À la mesure de la qualité du code ;
- À l'intégration continue des développements.

Transfert de connaissance

- Présenter à l'administration ou au titulaire entrant les processus dont notamment les processus propres au développement et au cycle projet, les processus de test, et de DevOps ;
- Organiser et animer des sessions de transfert d'acquis au profit des personnes désignées par l'administration.
- Assister le tiers repreneur à initialiser ses propres environnements de développement et de tests usine à iso socles techniques avec ses propres environnements.

Activité monitorée :

- Fournir des activités du maintien en conditions opérationnelles avec travail en parallèle pendant 1 mois du repreneur avec comparaison des livrables sans utilisation des livrables du repreneur ;
- Finaliser tout incident et problème, objet d'une intervention par le titulaire sortant ;
- Finaliser les demandes de maintenance évolutive en cours ;
- Le titulaire assure une maintenance monitorée auprès du repreneur, tout en gardant la responsabilité des livrables. La maintenance par le repreneur est progressive en termes de couverture technique et fonctionnelle, de criticité, de volume et de difficulté ;
- Le titulaire évalue les connaissances du repreneur

Transfert de responsabilité et bilan :

- Statuer sur la capacité du repreneur à passer en maintenance opérationnelle ;
- Accuser réception que le produit est totalement décommissionné dans les environnements techniques du titulaire (documentation, Forge, environnements applicatifs, jeux de données)
- Statuer sur l'éventuelle nécessité de prolonger l'activité monitorée.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit :

- La date de déclenchement de la phase de réversibilité et le déclenchement de la prestation correspondante ;
- La désignation du Chef de Projet en charge pour l'administration du bon déroulement et du suivi de la réversibilité ;
- La composition de l'équipe du nouvel entrant, et la désignation de son responsable.

TYPE DE PRIX

Cette prestation s'exécute sur quatre (4) mois au plus tard.

Il s'agit d'une prestation forfaitaire. Elle inclut l'ensemble des tâches et des livrables nécessaire à la bonne reprise du CBIMI par l'administration ou par un éventuel futur titulaire.

Cette prestation ne peut être commandée qu'une seule fois au cours de l'accord cadre.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

VIII. LOT 2 : FOURNITURE DES MIDDLEWARE MAINTENANCES ASSOCIEES ET EXPERTISES

VIII.1 PRESENTATION DU LOT 2

Le lot 2 a pour objet la fourniture de middleware, l'assistance à leur intégration et des expertises associées. Il inclut également une prestation de formation des équipes techniques et le cas échéant, la conception de nouvelles fonctionnalités non incluses dans la feuille de route de l'éditeur.

A noter que l'intégration au sein du système global du CBIMI des composants de ce lot sera assurée par le titulaire du lot 1 avec si besoin l'aide du titulaire du lot 2 par l'activation par l'administration des prestations « assistance et expertise » suivant le besoin.

Les prestations de ce lot seront exécutées dans le cadre du produit CBIMI mais d'autres périmètres applicatifs du ministère sont susceptibles d'utiliser ce marché pour faire l'acquisition de middleware. Il y a donc des besoins connus à date et des besoins encore inconnus tant pour le CBIMI que pour les autres périmètres du MI. Pour anticiper ces futurs besoins les natures des middleware listés vont donc au-delà des empreintes et de la prise d'image faciale.

Le lot 2 comprend six (6) prestations :

LOT 2	Fourniture des middleware, maintenances associées et expertises
Prestation L2P1	Fourniture de middleware et maintenances associées
Prestation L2P2	Fourniture de Dongles
Prestation L2P3	Assistance, expertises et formations
Prestation L2P4	Conception et développement de nouvelles fonctionnalités Middleware (hors roadmap éditeur)
Prestation L2P5	Réversibilité
Prestation L2P6	Transfert des licences Middleware sur un autre mode d'hébergement

VIII.2 DEFINITION

Les middleware sont des logiciels qui pilotent différents types de périphériques permettant de recueillir des données biométriques, de contrôler les périphériques, la qualité ou la cohérence des données recueillies et de les transmettre via API à l'application qui les a sollicitées.

Ils doivent :

- permettre le pilotage du capteur d'empreintes ;
- assurer un contrôle de biométrie standard ;
- permettre la lecture de document depuis une application web ;
- permettre la récupération des actions de captures et de contrôles effectués par le lecteur de document.

Les solutions middleware doivent par ailleurs :

- être conforme au socle de sécurité de l'administration et au CCT du ministère de l'intérieur,
- répondre au principe d'observabilité,
- être en conformité réglementaire avec les normes biométriques.

Le tableau suivant dresse la liste des typologies d'équipements que les middleware doivent pouvoir gérer de façon obligatoire ou facultative :

Fonction du middleware	Précision	Obligatoire (O) Facultatif (F)	PSE
Capture d'empreintes digitale	Mono doigts, Multi doigts Posé, Roulé	O	Non
Capture d'empreintes palmaire		F	Oui
Capture d'image faciale	Contrôle ICAO on / off	O	Non
Lecture de puce	Extraction des informations biométriques	O	Non
Capture d'iris		O	Non
Génétique / ADN		F	Oui
Enregistrement de la voix		F	Oui
Capture de la Signature		F	Oui
Capture de la Forme de la main		F	Oui
Capture du Réseaux veineux		F	Oui
Capture de la forme du Lobe de l'oreille		F	Oui
Capture de la Frappe au clavier		F	Oui
Capture de la Démarche		F	Oui
Lecture d'un QR Code		F	Oui
Scan de document		O	Non
Lecture de bande MRZ		O	Non
Lecture de fiche encrée		O	Non

VIII.3 NORMES APPLICABLES SUR LES COMPOSANTS BIOMETRIQUES

ICAO		Organisation de l'Aviation Civile Internationale : organisation internationale dont le rôle est de participer à l'élaboration des politiques et des normes qui permettent la standardisation du transport aéronautique international
ISO/IEC 10918	1994	Compression numérique et codage des images fixes (JPG)
ISO/IEC 15444-1	2019	Système de codage d'images JPEG 2000
ISO/IEC 19794-4	2011	Formats d'échange de données biométriques — Partie 5 : Données d'image du doigt (WSQ)
ISO/IEC 19794-5	2011	Formats d'échange de données biométriques — Partie 5 : Données d'image faciale
ISO/IEC 20027	2018	Profils biométriques interopérables - Recommandations pour les captures de 10 doigts à plat
ISO/IEC 20248	2018	Structures de données — Méta-structure de signature numérique
ISO/IEC 29794-4	2017	Qualité d'échantillon biométrique — Partie 4 : Données d'image de doigt (NFIQ2)
ISO/IEC 29794-5	2022	Qualité d'échantillon biométrique — Partie 5 : Données d'image de face
ISO/IEC 39794-4	2019	Formats extensibles d'échange de données biométriques — Partie 4 : Données d'image de doigt
ISO/IEC 39794-5	2019	Formats extensibles d'échange de données biométriques — Partie 5 : Données d'image faciale
FBI EBTS Appendix F		Appendice F de l'EBTS définissant les conditions de qualité d'image strictes, sur la comparaison des empreintes digitales et facilitant la correspondance 1 à N à grande échelle. Les capteurs certifiés FBI annexe F sont également considérés comme conforme aux spécifications PIV.
FBI PIV-071006		Norme de niveau inférieur conçue pour prendre en charge la vérification des empreintes digitales. (Personal Identity Verification IMAGE QUALITY SPECIFICATIONS FOR SINGLE FINGER CAPTURE DEVICES publié le 10/07/2006)
FIPS 140	2020	<i>Federal Information Processing Standards</i> : Ensemble de standards qui spécifient les exigences pour les modules de cryptographie.
Doc 9303	2021	Spécifications sur les documents de voyage lisibles à la machine, publié par l'ICAO, permettant à un État de faire reconnaître les documents d'identité comme documents de voyage valables par

		d'autres États ; Les documents doivent être conformes aux spécifications des Doc 9303-3 et Doc 9303-4, Doc 9303-5 ou Doc 9303-6.
NFIQ	2004	NIST Fingerprint Image Quality; mesure de la qualité d'image des empreintes digitales publié par le NIST
NFIQ 2	2021	NIST Fingerprint Image Quality 2 : logiciel open source de mesure de la qualité d'image des empreintes digitales, publié par la NIST et normalisé dans le cadre de la norme ISO/IEC 29794-4
ANSI/NIST-ITL-1	2015	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information : spécifie les formats à utiliser pour l'échange d'empreintes digitales et d'autres données d'image.
QSA		Evolution du logiciel standardisé open source prévue pour remplacer l'algorithme sFIQ propriétaire actuel utilisé pour le contrôle de la qualité des images faciales
AFNOR XP Z42-101	2019	Spécifications relatives à la mise en œuvre du CEV aux fins d'authentification, de vérification et d'acquisition de données véhiculées par un objet
AFNOR XP Z42-105	2020	Spécifications relatives à la mise en œuvre du CEV Otentik aux fins d'authentification, de vérification et de saisie automatique des données véhiculées par un document ou un objet
UE C 7774	2018	Spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres
UE C 7767	2018	Spécifications techniques du modèle uniforme de titre de séjour destiné aux ressortissants de pays tiers
UE 329	2019	Spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales et de l'image faciale aux fins de vérification et d'identification biométriques dans le système d'entrée/de sortie (EES)
OFIQ		https://github.com/BSI-OFIQ/OFIQ-Project implémentation de l'ISO 29794-5

VIII.4 ENVIRONNEMENTS DE FONCTIONNEMENT

Les middleware (ou logiciels intermédiaires) devront être compatibles avec Windows 10 et 11 (obligatoires), Ubuntu 64 bits et Android et Linux (en option pour ces trois derniers OS) et doivent pouvoir être déployés sur l'ensemble des postes de l'administration, et en interministériel (MEAE et DGDDI).

VIII.5 GESTION DES LICENCES

La gestion des licences relatives aux middleware (ou logiciels intermédiaires), peuvent être réalisées via des « dongles » ou via un serveur de licences en fonction de la solution retenue par l'administration.

- Deux modalités (2) de fourniture peuvent être demandées au titre de la prestation L2P1 par l'administration parmi lesquelles :

- **La fourniture de licences associées à des « dongles » (PSE):**

Dans ce cas, le titulaire doit fournir à l'administration :

- les licences dans les quantités commandées ;
- les numéros de licence associés aux numéros de « dongle », qui auront été fournis au préalable par l'administration qui assure l'inventaire de ces « dongles » et des licences ainsi que le suivi et la mise à jour de cet inventaire.

- **La fourniture de licences depuis un serveur hébergé par l'administration :**

Dans ce cas, le titulaire doit :

- mettre à disposition de l'administration un serveur de licences afin que les postes clients puisse s'y connecter et récupérer les jetons permettant l'utilisation du middleware ;
- assurer la maintenance de ce serveur de licences ;
- assurer la compatibilité de sa solution avec l'utilisation d'un serveur de licences.

Pour précision le serveur de licences mis à la disposition du titulaire doit pouvoir fonctionner sur le Cloud du ministère (de type OpenStack ou OpenShift avec de préférence le système d'exploitation Debian).

VIII.6 ÉQUIPE DU TITULAIRE

Pour réaliser les prestations du Lot 2, l'équipe du titulaire présente les profils et niveaux de séniorité suivants (le titulaire pourra proposer des profils complémentaires s'ils s'avèrent nécessaires à la réalisation des prestations) :

Lot 2	Séniorité exigée ³
Consultant technique	J, C, S, E
Développeur	J, C, S
Expert Biométrie	J,C,S,E

Le ministère autorise l'ajout de profils.

VIII.7 PRESTATION L2P1 - FOURNITURE DE MIDDLEWARE ET MAINTENANCES ASSOCIEES

OBJECTIFS DE LA PRESTATION

La présente prestation a pour objet de fournir à l'administration la concession des droits d'utilisation des middleware, lesquels doivent intégrer **l'ensemble des fonctionnalités identifiées comme obligatoires à l'article VIII.2.**

Les middleware fournis doivent permettre le **pilotage** des matériels existants listés ci-dessous ou, à défaut, indiquer le **délai nécessaire** pour assurer leur compatibilité :

- **Capteurs biométriques :**
MorphoTop100/100R, GreenBit DactyScan84c, Suprema, Morpho Top 20 20, capteur mono-doigt Morpho MSO331, dispositif nomade Morpho Mobile V3, Morpho Slim V3 ;
- **Lecteurs de documents :**
Elyctis ;
Lecteurs sécurisés Gemalto AT9000 MK2 et AT10K G ;
- **Lecteurs MRZ :**
Elyctis ID BOX One et modèle 141 ;
Gemalto ;
- **Scanners :**
Panasonic séries 25 et 26, Fujitsu, RICOH A6 modèle Fi-70f ;
- **Caméras :**
IDS UEye ;
Logitech Brio Ultra HD / 4K ;
Canon EOS R100 ;
- **Pad de signature :**
Wacom STU-430.

L'offre middleware du titulaire doit en outre pouvoir évoluer afin d'assurer la compatibilité avec l'évolution du parc d'équipements de l'administration.

La fourniture des middleware inclut en outre la réalisation des actions de maintenance corrective associées et leur maintien en condition de sécurité. Enfin la maintenance intègre la fourniture des évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes de qualité de biométrie et de mise en conformité réglementaire.

³ J : Junior, C : Confirmé, S : Sénior, E: Expert

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Il est entendu que les droits d'utilisation fournis au titre du marché incorporent :

- toutes évolutions et tous correctifs qui leur sont attachés ;
- les nouvelles versions.

Ces nouvelles versions doivent être préalablement soumises à l'accord de l'administration avant toute installation ou déploiement. Si l'administration refuse une nouvelle version (N+1) proposée par le titulaire, ce dernier est tenu de maintenir, aux conditions de l'accord-cadre, la version N en cours d'utilisation dans les services de l'administration jusqu'à la publication de la version suivante du composant par le titulaire (N+2). L'administration ne pourra refuser de mettre à jour une version N+2 par rapport à celle utilisée dans ces services.

Au titre de la fourniture des middleware les actions suivantes sont attendues :

Le titulaire doit fournir à l'administration :

- les droits d'utilisation nécessaires à la pleine utilisation des middleware ;
- la procédure d'installation des licences ;
- les mises à jour des middleware liées à des corrections ou évolutions : MCO, MCS, évolution produit, ect ;
- les nouvelles versions ;
- **les évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes biométriques et de mise en conformité réglementaire .**

Deux modalités (2) de fourniture peuvent être demandées par l'administration au titre de la prestation L2P1 parmi lesquelles :

- La fourniture de licences associées à des « dongles » (PSE):

Dans ce cas, le titulaire doit fournir à l'administration :

- les licences dans les quantités commandées ;
- les numéros de licence associés aux numéros de « dongle », les dongles sont fournis par le titulaire de l'accord-cadre en fonction du choix retenu par l'administration au titre de la L2P1. Celui-ci assure également l'inventaire de ces « dongles » et des licences ainsi que le suivi et la mise à jour de cet inventaire.

- La fourniture de licences depuis un serveur hébergé par l'administration

Dans ce cas, le titulaire doit :

- mettre à disposition de l'administration un serveur de licences afin que les postes clients puisse s'y connecter et récupérer les jetons permettant l'utilisation du middleware ;
- assurer la maintenance de ce serveur de licences ;
- assurer la compatibilité de sa solution avec l'utilisation d'un serveur de licences.

Pour précision le serveur de licences doit pouvoir fonctionner sur le Cloud du ministère (de type OpenStack ou OpenShift avec de préférence le système d'exploitation Debian).

Au titre de la L2P1, le titulaire assure également la maintenance corrective et le maintien en condition de sécurité des middleware :

Le titulaire doit :

- en cas de failles de sécurité sur un middleware, fournir à l'administration, les correctifs de sécurité à installer en ayant vérifié, au préalable, l'absence de régression sur le socle ;
- prendre en compte les constatations d'un dysfonctionnement établies et tracées par l'administration au travers d'une fiche d'incident ;

- fournir la solution de contournement ;
- réaliser l'analyse d'impact sur la mise en place du correctif ;
- établir le planning détaillé de mise à disposition du correctif ;
- réaliser les corrections et tests du socle (correctif, tests de non régression...),
- gérer les middleware en configuration ;
- livrer le correctif et la fiche de version contenant le script d'installation (du middleware ayant évolué ou du socle complet), les plans de tests et résultats de tests, la liste des anomalies corrigées ;
- fournir les informations nécessaires à l'élaboration de la fiche réflexe.

La fiche d'incident, renseignée dans l'applicatif de gestion des anomalies du titulaire contient :

- la nature de l'anomalie : bloquante, majeure ou mineure (Cf : définition documentée ci-dessous)
- l'identité et la localisation du demandeur ;
- le contexte de survenue de l'anomalie ;
- la description détaillée de l'anomalie, avec des copies d'écran le cas échéant ;
- date et heure de création, à partir desquelles les délais d'intervention du titulaire sont établis.

La criticité des anomalies est définie de la manière suivante :

- une anomalie est qualifiée de **bloquante** lorsqu'elle entraîne une perte totale ou partielle des services applicatifs réalisés par le, et concerne ainsi :
 - tout dysfonctionnement entraînant l'arrêt total d'une application ou d'un service applicatif,
 - toute anomalie qui rend impossible l'utilisation normale d'une fonctionnalité, de façon réversible et non contournable,
- une anomalie est qualifiée de **majeure** lorsqu'elle entraîne la dégradation d'un service applicatif en altérant le fonctionnement normal de l'application ou de l'une de ses fonctionnalités (du fait d'une erreur de cette dernière) mais sans empêcher l'utilisateur de dérouler un processus complet (i.e. pouvoir le terminer) ;
- une anomalie est qualifiée de **mineure** lorsqu'elle n'est pas désignée comme étant une anomalie bloquante ou majeure.

Le titulaire s'engage à respecter les délais maximums suivants (les délais exprimés courent à compter de la notification de l'incident par l'administration).

Catégorie d'incident	Bloquant	Majeur	Mineur
Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré
Solution de contournement	0,5 jour ouvré En cas d'incident signalé avant 12h : remise en état dans la journée. En cas d'incident après 12h: remise en état pour le lendemain avant 12h	Deux (2) jours ouvrés	Dix (10) jours ouvrés
Résolution par une solution pérenne	Cinq (5) jours ouvrés	Dix (10) jours ouvrés	Soixante-quinze (75) jours ouvrés

Le titulaire rédige et transmet le Plan d'Assurance (PAQ) et le Plan d'Assurance sécurité (PAS).

Sur demande de l'administration, des dongles ou un serveur de licence sera fourni au titulaire du lot 1 pour l'usage des logiciels sur ses environnements à des fins uniques de développement du CBIMI

PREREQUIS FOURNIS PAR L'ADMINISTRATION

- L'administration indique le mode de mise à disposition souhaité : **serveur de licence ou dongle**.
- En cas de fourniture de licences depuis un serveur hébergé par l'administration, celle-ci précise l'infrastructure pour la mise en place du serveur de licences.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé conformément à l'annexe financière sur un prix unitaire en fonction des paliers suivants et des modalités de déploiement indiquées.

Type de licence	Nombre d'utilisateurs
Fourniture de licences associées à des dongles	Entre 1 et 100
	Entre 101 et 500
	Entre 501 et 1000
	Entre 1001 et 2000
	Plus de 2 000
Fourniture de licences depuis un serveur hébergé par l'administration	Entre 1 et 100
	Entre 101 et 500
	Entre 501 et 1000
	Entre 1001 et 2000
	Plus de 2 000

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

VIII.8 PRESTATION L2P2 – FOURNITURE DE DONGLES GARANTIE STANDARD INCLUSE

OBJECTIFS DE LA PRESTATION

Cette prestation (PSE) a pour objet de permettre à l'administration d'acquérir des dongles de manière unitaire ou groupées en cas de perte, vol ou de détérioration dans l'hypothèse où les middlewares sont déployés via cette configuration.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Le titulaire fournit le dongle en y associant le middleware précédemment acquis par l'administration.

Au titre de la garantie incluse, titulaire est l'interlocuteur unique et exclusif des services de l'administration. Il est seul responsable de la parfaite conformité des prestations attachées à la

garantie pendant l'intégralité de leur période d'exécution. Par conséquent, il est interdit au titulaire d'orienter l'administration vers un constructeur, un sous-traitant ou un tiers mainteneur.

La garantie comprend : le dépannage par réparation ou remplacement des pièces ou sous-ensembles défectueux, usés ou cassés à la suite de l'usage conforme à la notice d'utilisation du matériel.

Sont exclus du service de garantie :

- ☐ la réparation des dommages ou défaillances du matériel résultant d'accidents ou de négligences non imputables au titulaire ou de l'accès frauduleux au matériel ;
- ☐ les conséquences de l'inobservation des conditions d'installation, d'environnement et d'utilisation ou des règles d'emploi du matériel ou de l'usage de courant électrique ou de fournitures ou de supports informatiques ne correspondant pas aux normes prescrites par le titulaire ;
- ☐ les extensions, connexions ou déconnexions non expressément prévues par le titulaire comme étant incluses dans le service ;
- ☐ la modification des matériels ou dispositifs à la demande de l'administration sauf lorsque ces modifications ont été réalisées par le titulaire.

A compter de la saisine du titulaire par l'administration celui-ci dispose d'un délai maximal de soixante (60) minutes pour confirmer la demande à l'administration. Cette confirmation revêt la forme d'un courriel adressé au service demandeur. S'agissant de la garantie standard et de l'extension de la garantie, le titulaire s'engage à une garantie de temps de rétablissement (GTR) fixée à dix (10) jours ouvrés maximum, retour dans les locaux de l'administration inclus, à compter de la demande d'intervention

PREREQUIS FOURNIS PAR L'ADMINISTRATION

Le périmètre de l'intervention, ainsi que sa durée, seront précisés par l'administration, lors de la commande.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur un prix unitaire conformément à l'annexe financière.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version validée par ses équipes.

VIII.9 L2P3 – ASSISTANCE, EXPERTISES ET FORMATIONS

OBJECTIFS DE LA PRESTATION

Cette prestation a pour objet de permettre au ministère de pouvoir bénéficier au sein de ses locaux en Île de France et hors Île de France de l'intervention d'un consultant (selon la nature de la demande) du titulaire de l'accord-cadre spécialisé sur l'un de ses produits afin de former le ministère, de présenter de nouvelles fonctionnalités, ou d'assister le ministère lors de son utilisation, son installation, la réalisation des tests de performance ou montée en charge.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Dans ce cas particulier, l'objectif est de viser des interventions relativement ciblées en termes de périmètre, et dont la durée est d'un (1) à dix (10) jours.

A ce titre, le titulaire apporte son assistance et son expertise (liste non exhaustive) sur :

- l'utilisation avancée des produits (configuration spécifique) ;
- la présentation avancée de nouvelles fonctionnalités ;
- l'optimisation de performances ;
- le soutien à l'organisation de tests de montée en charge.
- assistance au raccordement ou à l'intégration dans des systèmes tiers ;
- assistance à la mise en place de bouchons et/ou simulateurs ;
- expertise sur l'intégration des capteurs ;
- expertise sur les fonctionnalités des middleware ;
- aide au diagnostic vis-à-vis d'une application utilisant les middleware,

Expertise biométrie.

La prestation fait systématiquement l'objet d'un support et d'un compte-rendu d'intervention (CRI) qui a pour objet de recenser de manière synthétique les actions réalisées lors de la prestation.

Dans certains cas, la prestation pourra donner lieu à la fourniture d'une note d'information détaillée visant à préciser des modalités spécifiques d'utilisation de l'un des produits objet du présent marché dans le cadre d'utilisation propre au ministère.

Les procédures d'utilisation seront alors systématiquement remises au format PDF.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

Le périmètre de l'intervention, ainsi que sa durée, seront précisés par l'administration, lors de la commande. Sont précisés :

- le lieu d'exécution de la prestation ;
- le domaine d'expertise ;
- le périmètre de l'intervention et les livrables attendus ;
- les contraintes liées à l'objet de la mission ;
- le planning attendu de réalisation de la prestation.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur des unités d'œuvres (UO) selon une table des profils proposée et rappelant obligatoirement les travaux à réaliser, l'équipe et les livrables figurant au présent CCTP et le calendrier de réalisation.

Préalablement à toute intervention, le titulaire présentera à l'administration le profil et le CV de son intervenant pour validation.

Pour chaque commande de prestations exécutées hors Île France, le titulaire ajoute dans son devis le surcoût prévu pour le déplacement (prix 3.3 de l'annexe financière) et éventuellement le surcoût correspondant à l'hébergement et la restauration correspondant à la durée d'exécution (prix 3.3 de l'annexe financière).

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version validée par ses équipes.

VIII.10 PRESTATION L2P4 - CONCEPTION ET DEVELOPPEMENT DE NOUVELLES FONCTIONNALITES MIDDLEWARE (HORS ROADMAP EDETEUR)

OBJECTIFS DE LA PRESTATION

Cette prestation de conception et de développement consiste à créer de nouvelles fonctionnalités des middlewares non prévues initialement dans la feuille de route de l'éditeur ou réaliser des évolutions des middlewares existants.

Le développement se fait selon les prescriptions de l'administration dans la feuille de route du CBIMI.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation, il est attendu du titulaire au minimum les actions suivantes :

- Une analyse d'impact sur le ou les middlewares concerné(s) ;
- La conception technique détaillée de la fonctionnalité.

Le titulaire réalise les développements et tests permettant de garantir la conformité, et qualité de la fonctionnalité au besoin.

- développe les composants assortis de la typologie de tests réalisés et des tests de qualification et de non régression, gérés en configuration ;
- réalise et/ou maintient les scripts et outils permettant de réaliser les tests de charge et de performance ;
- met à jour l'ensemble de la documentation ;
- établit la fiche de livraison récapitulant le détail de la livraison .

A la demande de l'administration un support pourra être apporté concernant les déploiements applicatifs sur les différents environnements.

Chaque développement s'accompagne également d'une période de garantie d'un an au minimum pendant laquelle le titulaire réalise sans surcoût tout correctif de dysfonctionnement et le maintien en condition de sécurité du module ou de la fonctionnalité développée.

Il réalise ces correctifs et ce maintien en condition de sécurité selon les mêmes principes que ceux mis en place pour la fourniture des middleware (voir article VIII.7/VIII.7 partie " Au titre de la maintenance corrective et du maintien en condition de sécurité ») :

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit une expression de besoin de la fonctionnalité à développer avec le périmètre des équipements concernés complété d'un cas d'usage.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après

établissement d'un devis basé sur des unités d'œuvres (UO) selon une table des profils et rappelant obligatoirement les travaux à réaliser, l'équipe et les livrables figurant au présent CCTP et le calendrier de réalisation.

Préalablement à toute intervention, le titulaire présentera à l'administration le profil et le CV de son intervenant pour validation.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

VIII.11 PRESTATION L2P5 - REVERSIBILITE

OBJECTIFS DE LA PRESTATION

La réversibilité (ou transférabilité) a pour but d'organiser à l'issue de l'accord-cadre et sur le périmètre des développements spécifiques pour le ministère, un transfert de connaissances du titulaire à l'administration ou au bénéfice de toute autre personne désignée par l'administration ou de tout tiers désigné par celle-ci.

La réversibilité/transférabilité ne s'applique pas aux produits standards du titulaire mais seulement aux produits développés et propriété de l'administration.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Le titulaire assure, sur demande de l'administration et dans le délai imparti, une totale réversibilité/transférabilité des prestations de MCO/MCS et intégration des composants. Il s'interdit de faire obstacle à cette décision et s'engage à apporter toute l'assistance nécessaire à la bonne réalisation de cette opération tout en assurant la continuité de service.

La réversibilité/ transférabilité intervient soit dans le cas de la résiliation de l'accord-cadre soit à l'échéance de l'accord-cadre.

A ce titre, le titulaire :

- établit un plan de réversibilité/ transférabilité dans lequel il précise :
 - les rôles et responsabilités des interlocuteurs de l'administration du titulaire et du reprenant ;
 - les modalités de pilotage et de gestion des activités nécessaires au transfert de connaissance entre les acteurs ;
 - l'ensemble des éléments transférés dans leur dernière version (documents de conception, de réalisation d'installation, état des anomalies, etc.) ;
 - le planning de mise en œuvre de la réversibilité/ transférabilité ;
- assure le transfert de connaissances permettant à l'équipe du reprenant ou à l'administration de disposer de tous les éléments nécessaires à la reprise du périmètre ;
- forme l'équipe du reprenant ;
- assiste le reprenant ou l'administration lors de l'exécution de la reprise d'activité ;
- réalise le bilan de la réversibilité/transférabilité.

La réversibilité ou la transférabilité se déroule dans les locaux de l'administration.

Le titulaire nomme un responsable de la réversibilité/ transférabilité. Ce responsable est l'interlocuteur privilégié de l'administration, ou de ses représentants pendant cette période.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit :

- La date de début de la phase de réversibilité et le déclenchement de la prestation correspondante ;
- La désignation du Chef de Projet en charge pour l'administration du bon déroulement et du suivi de la réversibilité ;
- La composition de l'équipe du nouvel entrant, et la désignation de son responsable.

TYPE DE PRIX

La prestation de réversibilité est une prestation forfaitaire dont la durée est de trois (3) mois.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation.

VIII.12 PRESTATION L2P6 TRANSFERT DES LICENCES MIDDLEWARE SUR UN AUTRE MODE D'HEBERGEMENT

OBJECTIFS DE LA PRESTATION

Transférer les licences middleware sur un autre mode d'hébergement (PSE) dans le cas où l'administration décide de changer de mode de fourniture de licences.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation, il est attendu :

- De préparer la transition entre le mode initial de gestion des licences et le nouveau mode de licences en mettant en place les serveurs de licences nécessaires ou en assistant l'administration pour leur installation et leur configuration ;
- ou de fournir les caractéristiques techniques attendues des « dongles » si les licences y sont liées.

De plus, pendant cette phase, le titulaire doit continuer à :

- fournir à l'administration les droits d'utilisation nécessaires à la pleine utilisation des middleware;
- des droits d'utilisation illimités dans le temps quant à l'usage plein et entier des composants ; et cela, de manière à éviter tout blocage artificiel des dispositifs et des systèmes déployés au sein du ministère dans le temps ;
- assurer l'utilisation des middleware pendant une période de transition.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit une expression de besoin.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur un prix forfaitaire tel que renseigné dans l'annexe financière.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX. LOT 3 : FOURNITURE DES COMPOSANTS DU « NOYAU BIOMETRIQUE », ADJUDICATION, FOURNITURE DE SOLUTION DE CHIFFREMENT, MAINTENANCES ASSOCIEES ET EXPERTISES

IX.1 PRESENTATION DU LOT 3

La présente prestation a pour objet de fournir à l'administration les logiciels AFIS/ABIS nécessaires au « noyau biométrie », les fonctionnalités relatives au composant d'adjudication, et les solutions de chiffrement associées.

Cette prestation intègre par ailleurs des prestations de maintenance, visant à garantir la disponibilité, la performance et la sécurité continues de ces composants, en assurant sa mise à jour, sa correction des éventuelles anomalies et son adaptation aux évolutions technologiques.

A noter que l'intégration au sein du système global du CBIMI des composants de ce lot sera assurée par le titulaire du lot 1 avec si besoin l'aide du titulaire du lot 3 par l'activation par l'administration des prestations d'assistance et d'expertise suivant le besoin.

Les prestations de ce lot seront exécutées dans le cadre du produit CBIMI mais d'autres périmètres applicatifs de l'administration sont susceptibles d'utiliser ce marché pour faire l'acquisition des logiciels **éditeurs (AFIS ou ABIS et logiciel d'adjudication)**. Il y a donc des besoins connus à date et des besoins encore inconnus tant pour le CBIMI que pour les autres périmètres de l'administration.

Ce lot est composé de neuf (9) prestations :

LOT 3	Composants « noyau biométrie », adjudication, fourniture de solutions de chiffrement, maintenances associées et expertises
Prestation L3P1	Fourniture d'AFIS ou d'ABIS pour le composant « noyau biométrie » et maintenances associées
Prestation L3P2	Transfert des licences AFIS/ABIS sur un autre mode d'hébergement
Prestation L3P3	Fourniture du logiciel d'adjudication et maintenances associées
Prestation L3P4	Transfert des licences du logiciel d'adjudication sur un autre mode d'hébergement
Prestation L3P5	Solutions de chiffrement
Prestation L3P6	Assistance, expertises et formations pour l'ensemble des produits biométriques du lot 3
Prestation L3P7	Conception et développement de nouvelles fonctionnalités biométriques (hors roadmap éditeur) pour l'ensemble des produits biométriques du lot 3
Prestation L3P8	Fourniture de dongles garantie standard incluse
Prestation L3P9	Réversibilité

IX.2 GESTION DES LICENCES POUR LES AFIS/ ABIS ET LE LOGICIEL D'ADJUDICATION

La gestion des licences relatives aux AFIS ou ABIS pour le composant « noyau biométrie », et celle pour la fourniture du logiciel d'adjudication, peuvent être réalisées via des « dongles » ou via un serveur de licences en fonction de la solution retenue par l'administration.

Le cas échéant, si **les AFIS ou ABIS ou le logiciel d'adjudication** sont utilisés depuis un même poste de travail, le titulaire fera en sorte d'avoir un « dongle » unique permettant de décompter les licences utilisées.

Il en est de même pour les serveurs de licences où le titulaire fera en sorte d'avoir un serveur de licences pour l'ensemble des solutions couvertes par le présent lot tout en s'assurant que la gestion des licences puisse s'effectuer de manière séparée entre les différents produits biométriques du lot 3.

Pour les AFIS/ ABIS :

Deux modalités (2) de fourniture peuvent être demandées par l'administration parmi lesquelles :

- **La fourniture de licences associées à des « dongles (PSE) » :**

Dans ce cas, le titulaire doit fournir à l'administration :

- les licences dans les quantités commandées ;
- les numéros de licence associés aux numéros de « dongle », qui auront été fournis au préalable par l'administration qui assure l'inventaire de ces « dongles » et des licences ainsi que le suivi et la mise à jour de cet inventaire.

- **La fourniture de licences depuis un serveur hébergé par l'administration :**

Dans ce cas, le titulaire doit :

- mettre à disposition de l'administration un serveur de licences afin que les postes clients puisse s'y connecter et récupérer les jetons permettant l'utilisation des AFIS ou ABIS;
- assurer la maintenance de ce serveur de licences ;
- assurer la compatibilité de sa solution avec l'utilisation d'un serveur de licences.

Pour précision le serveur de licences doit pouvoir fonctionner sur le Cloud du ministère (de type OpenStack ou OpenShift avec de préférence le système d'exploitation Debian).

Pour le logiciel d'adjudication :

Deux modalités (2) de fourniture peuvent être demandées par l'administration parmi lesquelles :

- **La fourniture de licences associées à des « dongles (PSE) » :**

Dans ce cas, le titulaire doit fournir à l'administration :

- les licences dans les quantités commandées ;
- les numéros de licence associés aux numéros de « dongle », qui auront été fournis au préalable par l'administration qui assure l'inventaire de ces « dongles » et des licences ainsi que le suivi et la mise à jour de cet inventaire.

- **La fourniture de licences depuis un serveur hébergé par l'administration**

Dans ce cas, le titulaire doit :

- mettre à disposition de l'administration un serveur de licences afin que les postes clients puisse s'y connecter et récupérer les jetons permettant l'utilisation du logiciel d'adjudication;
- assurer la maintenance de ce serveur de licences ;
- assurer la compatibilité de sa solution avec l'utilisation d'un serveur de licences.

Pour précision le serveur de licences doit pouvoir fonctionner sur le Cloud du ministère (de type OpenStack ou OpenShift avec de préférence le système d'exploitation Debian).

Sur demande de l'administration, des dongles ou un serveur de licence sera fourni au titulaire du lot 1 pour l'usage des logiciels sur ses environnements à des fins uniques de développement du CBIMI.

IX.3 ÉQUIPE DU TITULAIRE

Pour réaliser les prestations du Lot 3, l'équipe du titulaire présente les profils et niveaux de séniorité suivants (le titulaire pourra proposer des profils complémentaires s'ils s'avèrent nécessaires à la réalisation des prestations) :

Lot 3	Séniorité exigée ⁴
Consultant technique	J, C, S, E
Développeur	J, C, S
Expert Biométrie	J,C ,S,E

Le ministère autorise l'ajout de profils.

IX.4 PRESTATION L3P1 - FOURNITURE D'AFIS OU D'ABIS POUR LE COMPOSANT « NOYAU BIOMETRIE » ET MAINTENANCES ASSOCIEES

OBJECTIFS DE LA PRESTATION

Cette prestation a pour objectif de fournir à l'administration la concession des droits d'utilisation propriétaire pour la durée totale de l'accord-cadre (reconduction comprise) nécessaires au fonctionnement et au déploiement du composant dit « noyau biométrie » nécessaire notamment au stockage et au Matching (AFIS/ABIS) du CBIMI.

Ce composant est présenté à l'article II.4 du présent CCTP.

Ce composant doit être instancié autant de fois que nécessaire en fonction des besoins de l'administration.

L'AFIS ou l'ABIS doit :

- fournir une réponse fluide et sans délai (inférieur à 5 secondes) lors de la recherche 1 :1 ou 1 : N,
- être conforme au socle de sécurité de l'administration et au CCT du ministère de l'intérieur (pour sa base de données, pouvoir fonctionner de façon préférentielle avec PostgreSQL et déployable sur le Cloud du **ministère OpenStack ou OpenShift avec de préférence le système d'exploitation Debian**),
- se compléter d'une solution permettant de lister le contenu de la base de données (pour la partie « inventaire » notamment). Idéalement, le titulaire fournit aussi un jeu d'APIs permettant de réaliser cette consultation via d'autres applications si nécessaire,
- répondre au principe d'observabilité,
- permettre la purge à partir d'une liste d'identifiants ou selon certains critères (date, statut des empreintes, ...),
- permettre une traçabilité des actions,
- être en conformité réglementaire avec les normes biométriques.

L'ABIS peut permettre une recherche multi-modale.

La fourniture d'AFIS ou d'ABIS inclut en outre la réalisation des actions de maintenance corrective associées et leur maintien en condition de sécurité. Enfin la maintenance intègre la fourniture des évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes de qualité de biométrie et de mise en conformité réglementaire.

Le titulaire rédige et transmet le Plan d'Assurance (PAQ) et le Plan d'Assurance sécurité (PAS).

4 J : Junior, C : Confirmé, S : Sénior, E: Expert

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Il est entendu que les droits d'utilisation fournis au titre du marché incorporent :

- toutes évolutions et tous correctifs qui leur sont attachés ;
- les nouvelles versions.

Ces nouvelles versions doivent être préalablement soumises à l'accord de l'administration avant toute installation ou déploiement. Si l'administration refuse une nouvelle version (N+1) proposée par le titulaire, ce dernier est tenu de maintenir, aux conditions de l'accord-cadre, la version N en cours d'utilisation dans les services de l'administration jusqu'à la publication de la version suivante du composant par le titulaire (N+2). L'administration ne pourra refuser de mettre à jour une version N+2 par rapport à celle utilisée dans ces services.

Le titulaire fournit des composants permettant de couvrir les fonctionnalités exposées à l'article II.4 du présent CCTP.

Au titre de la fourniture des AFIS et ABIS les actions suivantes sont attendues :

Le titulaire doit fournir à l'administration :

- les droits d'utilisation nécessaires à la pleine utilisation des AFIS ou ABIS ;
- la procédure d'installation des licences ;
- toutes évolutions et tous correctifs qui leur sont attachés ;
- **les évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes biométriques et de mise en conformité réglementaire ;**
- Les nouvelles versions.
- les mises à jour des AFIS ou ABIS liées à des corrections ou évolutions : MCO, MCS, évolution produit, ect.

Le titulaire assure également :

- la gestion des obsolescences de composants logiciels ;
- les mises à jour de sécurité ;
- la mise à niveau des versions logicielles ;
- l'évolution des produits d'éditeurs tiers, changement de versions d'OS, etc ;
- le changement de version de tout élément de langage utilisé pour le développement logiciel (ex. changement de version de Java) ;
- le remplacement d'une brique logicielle par une autre technologie le cas échéant.

Chaque composant s'accompagne d'une documentation d'utilisation, d'installation, de configuration, d'intégration et de paramétrage en français, et des prérequis techniques de fonctionnement associés.

Au titre de la maintenance corrective et du maintien en condition de sécurité :

Le titulaire doit :

- en cas de failles de sécurité sur ses solutions , fournir à l'administration, les correctifs de sécurité à installer en ayant vérifié, au préalable, l'absence de régression sur le socle ;
- prendre en compte les constatations d'un dysfonctionnement établies et tracées par l'administration au travers d'une fiche d'incident ;
- fournir la solution de contournement ;
- réaliser l'analyse d'impact sur la mise en place du correctif ;
- établir le planning détaillé de mise à disposition du correctif ;
- réaliser les corrections et tests du socle (correctif, tests de non régression...),
- gérer les AFIS et ABIS en configuration ;

- livrer le correctif et la fiche de version contenant le script d'installation, les plans de tests et résultats de tests, la liste des anomalies corrigées ;
- fournir les informations nécessaires à l'élaboration de la fiche réflexe.

Le titulaire propose une solution en ligne de gestion des anomalies permettant à l'administration de renseigner des fiches d'incident avec les informations suivantes :

- la nature de l'anomalie : bloquante, majeure ou mineure ;
- service concerné ; ;
- le contexte de survenue de l'anomalie ;
- la description détaillée de l'anomalie, avec des copies d'écran le cas échéant ;
- date et heure de création, à partir desquelles les délais d'intervention du titulaire sont établis.

La criticité des anomalies est définie de la manière suivante :

- une anomalie est qualifiée de **bloquante** lorsqu'elle entraîne une perte totale ou partielle des services applicatifs réalisés par le titulaire
- et concerne ainsi :
 - tout dysfonctionnement entraînant l'arrêt total d'une application ou d'un service applicatif,
 - toute anomalie qui rend impossible l'utilisation normale d'une fonctionnalité, de façon réductible et non contournable,
- une anomalie est qualifiée de **majeure** lorsqu'elle entraîne la dégradation d'un service applicatif en altérant le fonctionnement normal de l'application ou de l'une de ses fonctionnalités (du fait d'une erreur de cette dernière) mais sans empêcher l'utilisateur de dérouler un processus complet (i.e. pouvoir le terminer) ;
- une anomalie est qualifiée de **mineure** lorsqu'elle n'est pas désignée comme étant une anomalie bloquante ou majeure.

Le titulaire s'engage à respecter les délais maximums suivants (les délais exprimés courent à compter de la notification de l'incident par l'administration).

Catégorie d'incident	Bloquant	Majeur	Mineur
Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré
Solution de contournement	0,5 jour ouvré En cas d'incident signalé avant 12h : remise en état dans la journée. En cas d'incident après 12h: remise en état pour le lendemain avant 12h	Deux (2) jours ouvrés	Dix (10) jours ouvrés
Résolution par une solution pérenne	Cinq (5) jours ouvrés	Dix (10) jours ouvrés	Soixante-quinze (75) jours ouvrés

PREREQUIS FOURNIS PAR L'ADMINISTRATION

- En cas de fourniture de licence avec dongle, l'administration indique les numéros de dongle.

- En cas de fourniture de licences depuis un serveur hébergé par l'administration, celle-ci précise l'infrastructure pour la mise en place du serveur de licences.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé conformément à l'annexe financière sur un prix unitaire en fonction des paliers suivants et des modalités de déploiement indiquées :

Type de licence AFIS et/ ou ABIS	Nombre d'enregistrements
Fourniture de licences associées à des dongles Licences avec dongle (PSE)	Entre 0 et 500 000
	Entre 500 001 et 1 million
	Entre 1 million et 3 millions
	Entre 3 millions et 6 millions
	Entre 6 millions et 10 millions
Fourniture de licences depuis un serveur hébergé par l'administration	Entre 0 et 500 000
	Entre 500 001 et 1 million
	Entre 1 million et 3 millions
	Entre 3 millions et 6 millions
	Entre 6 millions et 10 millions
Fourniture additionnelle de capacité de L'AFIS	Augmentation de la capacité de 1 million
Fourniture additionnelle de capacité de L'ABIS	Augmentation de la capacité de 1 million

La licence d'utilisation de l'AFIS et/ou de l'ABIS sont acquises en fonction d'un dimensionnement tel que mentionné en supra et dans l'annexe financière. Au besoin, l'administration pourra augmenter la capacité de l'AFIS et/ ou de l'ABIS par pallier de 1 million.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.5 PRESTATION L3P2 TRANSFERT DES LICENCES AFIS/ABIS SUR UN AUTRE MODE D'HEBERGEMENT

OBJECTIFS DE LA PRESTATION

Transférer les licences AFIS/ABIS (PSE) sur un autre mode d'hébergement. Dans le cas où l'administration décide de changer de mode de fourniture de licences.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation, il est attendu :

- De préparer la transition entre le mode initial de gestion des licences et le nouveau mode de licences en mettant en place les serveurs de licences nécessaires ou en assistant l'administration pour leur installation et leur configuration ;
- ou de fournir les caractéristiques techniques attendues des « dongles » si les licences y sont liées.

De plus, pendant cette phase, le titulaire doit continuer à :

<ul style="list-style-type: none"> fournir à l'administration les droits d'utilisation nécessaires à la pleine utilisation des AFIS/ABIS; des droits d'utilisation illimités dans le temps quant à l'usage plein et entier des composants ; et cela, de manière à éviter tout blocage artificiel des dispositifs et des systèmes déployés au sein du ministère dans le temps ; assurer l'utilisation des middleware pendant une période de transition.
PREREQUIS FOURNIS PAR L'ADMINISTRATION
L'administration fournit une expression de besoin.
TYPE DE PRIX
Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur un prix forfaitaire tel que renseigné dans l'annexe financière.
LIVRABLES
La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.6 PRESTATION L3P3 - FOURNITURE DU LOGICIEL D'ADJUDICATION ET MAINTENANCES ASSOCIEES

OBJECTIFS DE LA PRESTATION
<p>Cette prestation a pour objet de fournir à l'administration le composant d'adjudication du CBIMI et la maintenance associée à l'exécution conforme aux attentes de l'administration du composant.</p> <p>Le composant d'adjudication permet de procéder à la confirmation de l'identification et l'authentification des personnes de manière fiable, en fonction de caractéristiques biologiques uniques (données biométriques).</p> <p>Il permet à l'adjudicateur, d'enregistrer une décision « match ou no match » pour chaque personne, dans une liste de recherche.</p> <p>Les fonctionnalités d'adjudication suivantes sont également possibles :</p> <ul style="list-style-type: none"> semi-automatique (adjudication automatique au-dessus d'un seuil de confiance fixé), multimodale, pour tout type de données biométriques, <p>Le logiciel d'adjudication doit :</p> <ul style="list-style-type: none"> être conforme au socle de sécurité de l'administration et au CCT du ministère de l'intérieur déployable sur le Cloud du ministère OpenStack ou OpenShift avec de préférence le système d'exploitation Debian, répondre au principe d'observabilité, permettre une traçabilité des actions, être en conformité réglementaire avec les normes biométriques. <p>La fourniture du composant d'adjudication inclut en outre la réalisation des actions de maintenance corrective associées et leur maintien en condition de sécurité. Enfin la maintenance intègre la</p>

fourniture des évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes de qualité de biométrie et de mise en conformité réglementaire.

Le titulaire rédige et transmet le Plan d'Assurance (PAQ) et le Plan d'Assurance sécurité (PAS).

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Il est entendu que les droits d'utilisation fournis au titre du marché incorporent :

- toutes évolutions et tous correctifs qui leur sont attachés ;
- les nouvelles versions.

Ces nouvelles versions doivent être préalablement soumises à l'accord de l'administration avant toute installation ou déploiement. Si l'administration refuse une nouvelle version (N+1) proposée par le titulaire, ce dernier est tenu de maintenir, aux conditions de l'accord-cadre, la version N en cours d'utilisation dans les services de l'administration jusqu'à la publication de la version suivante du composant par le titulaire (N+2). L'administration ne pourra refuser de mettre à jour une version N+2 par rapport à celle utilisée dans ces services.

Au titre de la fourniture du composant d'adjudication

Le titulaire doit fournir à l'administration :

- les droits d'utilisation nécessaires à la pleine utilisation du logiciel d'adjudication ;
- la procédure d'installation des licences ;
- toutes évolutions et tous correctifs qui leur sont attachés ;
- **les évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes biométriques et de mise en conformité réglementaire ;**
- Les nouvelles versions.
- les mises à jour du logiciel d'adjudication liées à des corrections ou évolutions : MCO, MCS, évolution produit, ect

Au titre de la maintenance corrective et du maintien en condition de sécurité :

Le titulaire doit :

- en cas de failles de sécurité sur ses solutions , fournir à l'administration, les correctifs de sécurité à installer en ayant vérifié, au préalable, l'absence de régression sur le socle ;
- prendre en compte les constatations d'un dysfonctionnement établies et tracées par l'administration au travers d'une fiche d'incident ;
- fournir la solution de contournement ;
- réaliser l'analyse d'impact sur la mise en place du correctif ;
- établir le planning détaillé de mise à disposition du correctif ;
- réaliser les corrections et tests du socle (correctif, tests de non régression...),
- gérer le composant d'adjudication en configuration ;
- livrer le correctif et la fiche de version contenant le script d'installation, les plans de tests et résultats de tests, la liste des anomalies corrigées ;
- fournir les informations nécessaires à l'élaboration de la fiche réflexe.

Le titulaire propose une solution en ligne de gestion des anomalies permettant à l'administration de renseigner des fiches d'incident avec les informations suivantes :

- la nature de l'anomalie : bloquante, majeure ou mineure ;
- l'identité et la localisation du demandeur ;
- le contexte de survenue de l'anomalie ;
- la description détaillée de l'anomalie, avec des copies d'écran le cas échéant ;
- date et heure de création, à partir desquelles les délais d'intervention du titulaire sont établis.

La criticité des anomalies est définie de la manière suivante :

- une anomalie est qualifiée de **bloquante** lorsqu'elle entraîne une perte totale ou partielle des services applicatifs réalisés par le titulaire et concerne ainsi :
 - tout dysfonctionnement entraînant l'arrêt total d'une application ou d'un service applicatif,
 - toute anomalie qui rend impossible l'utilisation normale d'une fonctionnalité, de façon rédhibitoire et non contournable,
- une anomalie est qualifiée de **majeure** lorsqu'elle entraîne la dégradation d'un service applicatif en altérant le fonctionnement normal de l'application ou de l'une de ses fonctionnalités (du fait d'une erreur de cette dernière) mais sans empêcher l'utilisateur de dérouler un processus complet (i.e. pouvoir le terminer) ;
- une anomalie est qualifiée de **mineure** lorsqu'elle n'est pas désignée comme étant une anomalie bloquante ou majeure.

Le titulaire s'engage à respecter les délais maximums suivants (les délais exprimés courent à compter de la notification de l'incident par l'administration).

Catégorie d'incident	Bloquant	Majeur	Mineur
Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré
Solution de contournement	0,5 jour ouvré En cas d'incident signalé avant 12h : remise en état dans la journée. En cas d'incident après 12h: remise en état pour le lendemain avant 12h	Deux (2) jours ouvrés	Dix (10) jours ouvrés
Résolution par une solution pérenne	Cinq (5) jours ouvrés	Dix (10) jours ouvrés	Soixante-quinze (75) jours ouvrés

PREREQUIS FOURNIS PAR L'ADMINISTRATION

- En cas de fourniture de licence avec dongle, l'administration indique les numéros de dongle.
- En cas de fourniture de licences depuis un serveur hébergé par l'administration, celle-ci précise l'infrastructure pour la mise en place du serveur de licences.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé conformément à l'annexe financière sur un prix unitaire en fonction des paliers suivants et des modalités de déploiement indiquées :

Type de licence	Nombre d'utilisateurs
-----------------	-----------------------

	Fourniture de licences associées à des dongles	Entre 1 et 10	
		Entre 11 et 50	
		Entre 51 et 100	
		Entre 101 et 200	
		Entre 201 et 500	
	Fourniture de licences depuis un serveur hébergé par l'administration	Entre 1 et 10	
		Entre 11 et 50	
		Entre 51 et 100	
		Entre 101 et 200	
		Entre 201 et 500	

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.7 PRESTATION L3P4 TRANSFERT DES LICENCES DU LOGICIEL D'ADJUDICATION SUR UN AUTRE MODE D'HEBERGEMENT

OBJECTIFS DE LA PRESTATION

Transférer les licences d'adjudication sur un autre mode d'hébergement. Dans le cas où l'administration décide de changer de mode de fourniture de licences.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation (PSE), il est attendu :

- De préparer la transition entre le mode initial de gestion des licences et le nouveau mode de licences en mettant en place les serveurs de licences nécessaires ou en assistant l'administration pour leur installation et leur configuration ;
- Ou de fournir les caractéristiques techniques attendues des « dongles » si les licences y sont liées.

De plus, pendant cette phase, le titulaire doit continuer à :

- fournir à l'administration les droits d'utilisation nécessaires à la pleine utilisation du module d'adjudication.
- des droits d'utilisation illimités dans le temps quant à l'usage plein et entier des composants ; et cela, de manière à éviter tout blocage artificiel des dispositifs et des systèmes déployés au sein du ministère dans le temps ;
- assurer l'utilisation du module d'adjudication pendant une période de transition.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit une expression de besoin.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur un prix forfaitaire tel que renseigné dans l'annexe financière.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.8 PRESTATION L3P5 - FOURNITURE DE SOLUTIONS DE CHIFFREMENT ET MAINTENANCES ASSOCIEES

OBJECTIFS DE LA PRESTATION, DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Cette prestation a pour objectif de fournir à l'administration les solutions de chiffrement nécessaires au fonctionnement de la solution du CBIMI afin de protéger le lien entre les données alphanumériques et des données biométriques. Les solutions de chiffrement proposées au titre de la L3P5-du présent lot 3 et intègre un SLA à 99% que la solution soit matérielle ou logicielle.

La solution doit être en capacité de générer, stocker et protéger des clefs cryptographiques ainsi que les maintenances associées. Ce matériel est fourni sous la forme d'une **solution matérielle ou d'une solution logicielle en fonction du choix retenu par l'administration.**

Pour le chiffrement matériel il s'agit d'un « Hardware Security Module » **(ci-après boîtiers HSM)** ou d'une solution virtualisée, **logicielle de chiffrement.**

Cette fourniture incorpore une garantie standard et peut faire l'objet d'une extension de garantie pour **les HSM.**

S'agissant de la solution virtualisée, la fourniture du logicielle de chiffrement inclut en outre la réalisation des actions de maintenance corrective associées et leur maintien en condition de sécurité. Enfin la maintenance intègre la fourniture des évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes de sécurité et d'accessibilité de type ANSSI, eIDAS et de mise en conformité réglementaire.

Elle se compose de trois (3) sous-prestations :

Sous prestation 5.1 : Fourniture de boîtier HSM (garantie standard inclus)

Sous-prestation 5.2 : Extension de garantie relative au boîtier HSM

Sous prestation 5.3 : Fourniture d'une solution logicielle de chiffrement et maintenances associées.

La solution de chiffrement matérielle ou logicielle doit permettre le chiffrement du lien entre les données alphanumériques et les données biométriques.

Le titulaire fournit des solutions de chiffrement logicielles ou matérielles répondant aux exigences fonctionnelles et techniques ci-dessous :

- Sécurité des clés cryptographiques,
- Résistance aux attaques physiques,
- Conformité réglementaire,
- Performance,
- Gestion des Accès et Contrôle d'Intégrité (AIDE),
- Fiabilité.

Le titulaire doit mettre à disposition de l'administration des solutions de chiffrement respectant les principes suivants :

- **L'observabilité** : mesure et analyses des données offrant une vue détaillée de l'état et des performances du système (monitoring, métriques, logs, traces).

- **La tenue d'une piste d'audit :** toute opération est tracée et liée à l'identité de l'accédant qui en est à l'origine, de sorte que le comportement du système global reste observable et que l'administration soit en mesure de détecter des comportements anormaux, même lorsque plusieurs services sont impliqués.

Contenu de la garantie standard des HSM :

S'agissant des conditions et des modalités pratiques d'exécution de la garantie et de maintenance, quel qu'en soit le type, le titulaire de l'accord-cadre est l'interlocuteur unique et exclusif des services de l'administration. Il est seul responsable de la parfaite conformité des prestations attachées à la garantie pendant l'intégralité de leur période d'exécution. Par conséquent, il est interdit au titulaire d'orienter l'administration vers un constructeur, un sous-traitant ou un tiers mainteneur. La garantie s'entend avec l'obligation de résultat.

Les caractéristiques de la garantie sont les suivantes :

- s'agissant de la garantie standard incorporée à l'acquisition des matériels, celle-ci est limitée au contenu de la garantie constructeur, c'est-à-dire à une garantie pièces ;
- dans tous les cas, une adresse électronique pour déposer les demandes d'intervention.
- le service de garantie des matériels inclut :
 - le dépannage par réparation ou remplacement des pièces ou sous-ensembles défectueux, usés ou cassés à la suite de l'usage conforme à la notice d'utilisation du matériel ;
 - le contrôle du bon état technique du matériel, à l'occasion des interventions du titulaire ;
- tous les composants internes commandés en même temps qu'un matériel bénéficient automatiquement de la garantie de celui-ci.
- pour tous les matériels objets de la garantie, les pièces de rechange nécessaires à l'application de la garantie sont disponibles pendant toute la durée de celle-ci.

Exclusion de garantie :

Sont exclus du service de garantie :

- la réparation des dommages ou défaillances du matériel résultant d'accidents ou de négligences non imputables au titulaire ou l'accès frauduleux au matériel ;
- les conséquences de l'inobservation des conditions d'installation, d'environnement et d'utilisation ou des règles d'emploi du matériel ou de l'usage de courant électrique ou de fournitures ou de supports informatiques ne correspondant pas aux normes prescrites par le titulaire ;
- la modification des matériels ou dispositifs à la demande de l'administration sauf lorsque ces modifications ont été réalisées par le titulaire.

Modalités d'exécution de la garantie :

Pour l'exécution conforme de la garantie, le titulaire est tenu de fournir à l'administration une adresse électronique comme moyen de déclenchement de la garantie.

Le moyen de déclenchement est disponible les jours ouvrés de l'administration, de 9h00 à 18h30. Le fuseau horaire utilisé est celui de la France métropolitaine.

Dans le cas où le retour d'un matériel défectueux en France est nécessaire, le titulaire met tout en œuvre pour préparer et envoyer un matériel de remplacement dans les délais les plus brefs, sans attendre la réception du matériel retourné.

Extension de garantie sur les HSM :

Cette sous-prestation consiste à fournir une extension de garantie (pièces, main d'œuvre niveau de service, mise à jour logiciel,) pour les boîtiers HSM.

Le contenu de cette extension est au minimum équivalent aux dispositions de la garantie initiale.

L'extension de garantie visée concerne en particulier la gestion des réparations matérielles des boîtiers HSM. Elle inclut au minimum :

- le maintien en condition opérationnelle (MCO) des boîtiers HSM ;
- leur réparation, mise à jour ou leur remplacement si nécessaire ;
- la livraison des pièces de rechange en France métropolitaine et/ ou la mise à disposition de la solution logicielle de chiffrement ;

Le titulaire réalise les diagnostics appropriés, y compris en se déplaçant sur le site de l'administration si nécessaire, et assure les réparations ou le remplacement de l'équipement le cas échéant.

Tous les frais de transport des équipements, aller-retour, entre le site de l'administration et celui du titulaire sont à la charge de ce dernier.

EXIGENCES DE SERVICES RELATIVE AU HSM

Assistance téléphonique :

9h00 – 18H00 du lundi au vendredi (jours ouvrés)

Enregistrement des demandes via une plateforme de demande et ou assistance par e-mail

9h00 – 18H00 du lundi au vendredi (jours ouvrés)

Délai de réponse maximale de **5 heures** à la requête initiale

Capitalisation des anomalies et aide à détection des problèmes au travers d'un outil d'observabilité

Remplacement anticipé du matériel défectueux (sans avoir préalablement retourné le matériel défaillant). Processus : A l'issue d'une qualification d'anomalie par le titulaire confirmant la décision de remplacement du matériel, un nouvel HSM est envoyé par transporteur à **J+3** sur le site de l'administration en région parisienne.

La prestation inclut les mises à jour des firmwares et du logiciel ; dès disponibilité.

La prestation inclut les correctifs pour les problèmes de micrologiciel

Retourner le matériel défectueux pour réparation ou remplacement (délai de 15 jours)

Les matériels sont livrés en France métropolitaine et Corse comprise, à l'adresse indiquée dans le bon de commande.

Le délai d'exécution de la prestation est d'un (1) mois calendaire à compter de la notification du bon de commande

Au titre de la fourniture d'une solution logicielle de chiffrement ::

Il est entendu que les droits d'utilisation fournis au titre du marché incorporent :

- les droits d'utilisation nécessaires à la pleine utilisation du logiciel de chiffrement;
- la procédure d'installation des licences ;
- toutes évolutions et tous correctifs qui leur sont attachés ;
- **les évolutions et adaptations fonctionnelles requises par les évolutions et nouvelles normes et de mise en conformité réglementaire ;**
- Les nouvelles versions.
- les mises à jour du logiciel de chiffrement liées à des corrections ou évolutions : MCO, MCS, évolution produit, ect

Ces nouvelles versions doivent être préalablement soumises à l'accord de l'administration avant toute installation ou déploiement. Si l'administration refuse une nouvelle version (N+1) proposée par le titulaire, ce dernier est tenu de maintenir, aux conditions de l'accord-cadre, la version N en cours d'utilisation dans les services de l'administration jusqu'à la publication de la version suivante du composant par le titulaire (N+2). L'administration

Le titulaire fournit des composants permettant de couvrir les fonctionnalités exposées à l'article II.5 du présent CCTP.

A ce titre, le titulaire doit fournir à l'administration :

- les droits d'utilisation nécessaires à la pleine utilisation de ses solutions;
- des droits d'utilisation illimités dans le temps quant à l'usage plein et entier des composants ; et cela, de manière à éviter tout blocage artificiel des dispositifs et des systèmes déployés au sein du ministère dans le temps ;
- les licences dans les quantités commandées ;
- la procédure d'installation des licences ;
- les mises à jour liées à des corrections ou évolutions.

Le titulaire assure également :

- la gestion des obsolescences de composants logiciels ;
- les mises à jour de sécurité ;
- la mise à niveau des versions logicielles ;
- l'évolution des produits d'éditeurs tiers, changement de versions d'OS, etc ;
- le changement de version de tout élément de langage utilisé pour le développement logiciel (ex. changement de version de Java) ;
- le remplacement d'une brique logicielle par une autre technologie le cas échéant.

Chaque composant s'accompagne d'une documentation d'utilisation, d'installation, de configuration, d'intégration et de paramétrage en français, et des prérequis techniques de fonctionnement associés.

Au titre de la maintenance corrective et du maintien en condition de sécurité :

Le titulaire doit :

- en cas de failles de sécurité, fournir à l'administration, les correctifs de sécurité à installer en ayant vérifié, au préalable, l'absence de régression ;
- prendre en compte les constatations d'un dysfonctionnement établies et tracées par l'administration au travers d'une fiche d'incident ;
- fournir la solution de contournement ;
- réaliser l'analyse d'impact sur la mise en place du correctif ;
- établir le planning détaillé de mise à disposition du correctif ;
- réaliser les corrections et tests
- gérer la solution de chiffrement en configuration ;
- livrer le correctif et la fiche de version contenant le script d'installation, les plans de tests et résultats de tests, la liste des anomalies corrigées ;

La fiche d'incident, renseignée dans l'appliquatif de gestion des anomalies du titulaire contient :

- la nature de l'anomalie : bloquante, majeure ou mineure (Cf : définition documentée ci-dessous)
- l'identité et la localisation du demandeur ;
- le contexte de survenue de l'anomalie ;
- la description détaillée de l'anomalie, avec des copies d'écran le cas échéant ;
- date et heure de création, à partir desquelles les délais d'intervention du titulaire sont établis.

La criticité des anomalies est définie de la manière suivante :

- une anomalie est qualifiée de **bloquante** lorsqu'elle entraîne une perte totale ou partielle des services applicatifs réalisés par le titulaire :
 - tout dysfonctionnement entraînant l'arrêt total d'une application ou d'un service applicatif,
 - toute anomalie qui rend impossible l'utilisation normale d'une fonctionnalité, de façon rédhibitoire et non contournable,
- une anomalie est qualifiée de **majeure** lorsqu'elle entraîne la dégradation d'un service applicatif en altérant le fonctionnement normal de l'application ou de l'une de ses fonctionnalités (du fait d'une erreur de cette dernière) mais sans empêcher l'utilisateur de dérouler un processus complet (i.e. pouvoir le terminer) ;
- une anomalie est qualifiée de **mineure** lorsqu'elle n'est pas désignée comme étant une anomalie bloquante ou majeure.

Le titulaire s'engage à respecter les délais maximums suivants (les délais exprimés courent à compter de la notification de l'incident par l'administration).

Catégorie d'incident	Bloquant	Majeur	Mineur
Temps de réponse	Une (1) heure ouvrée	Quatre (4) heures ouvrées	Un (1) jour ouvré
Solution de contournement	0,5 jour ouvré En cas d'incident signalé avant 12h : remise en état dans la journée. En cas d'incident après 12h : remise en état pour le lendemain avant 12h	Deux (2) jours ouvrés	Dix (10) jours ouvrés

Point d'attention : toute solution logicielle qui consiste à réaliser le chiffrement sur une plate-forme externe à celle de l'administration est proscrite.

Le titulaire rédige et transmet le Plan d'Assurance (PAQ) et le Plan d'Assurance sécurité (PAS) en fonction de la solution retenue par l'administration et met à disposition un outil d'observabilité.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit les caractéristiques des solutions de chiffrement et les modalités de mise à disposition attendues et l'adresse de livraison des boîtiers HSM le cas échéant

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande sur la base d'un prix unitaire conformément à l'annexe financière.

Solution attendue	Type de prix
Boîtier HSM	Unitaire par boîtier
Solution de chiffrement logicielle et maintenances associées	Unitaire
Extension de garantie d'un boîtier	Extension annuelle

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.9 PRESTATION L3P6 – ASSISTANCE, EXPERTISES ET FORMATIONS POUR L'ENSEMBLE DES PRODUITS BIOMETRIQUES DU LOT 3

OBJECTIFS DE LA PRESTATION

Cette prestation a pour objet de permettre au ministère de pouvoir bénéficier au sein de ses locaux en île-de-France ou hors île-de-France de l'intervention d'un expert ou consultant confirmé (selon la nature de la demande) du titulaire de l'accord-cadre spécialisé sur **l'ensemble des produits du lot 3** afin de former le ministère, de présenter de nouvelles fonctionnalités, ou d'assister le ministère lors de son utilisation, son installation, la réalisation des tests de performance ou montée en charge.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Dans ce cas particulier, l'objectif est de viser des interventions relativement ciblées en terme de périmètre, et dont la durée est d'un (1) à dix (10) jours.

A ce titre, le titulaire apporte son expertise (liste non exhaustive) sur :

- l'utilisation avancée des produits (configuration spécifique) ;
- la présentation avancée de nouvelles fonctionnalités ;
- l'optimisation de performances ;
- le soutien à l'organisation de tests de montée en charge.
- assistance au raccordement ou à l'intégration dans des systèmes tiers ;
- assistance à la mise en place de bouchons et/ou simulateurs ;
- expertise sur les fonctionnalités des composants du présent lot ;
- aide au diagnostic vis-à-vis d'une application utilisant l'un des composants du présent lot.
- Expertise biométrie.

La prestation fait systématiquement l'objet d'un support et d'un compte-rendu d'intervention (CRI) qui a pour objet de recenser de manière synthétique les actions réalisées lors de la prestation.

Dans certains cas, la prestation pourra donner lieu à la fourniture d'une note d'information détaillée visant à préciser des modalités spécifiques d'utilisation de l'un des produits objet du présent marché dans le cadre d'utilisation propre au ministère.

Les procédures seront alors systématiquement remises au format PDF.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

Le périmètre de l'intervention, ainsi que sa durée, seront précisés par l'administration, lors de la commande. Sont précisés :

- le lieu d'exécution de la prestation ;
- le domaine d'expertise ;
- le périmètre de l'intervention et les livrables attendus ;
- les contraintes liées à l'objet de la mission ;
- le planning attendu de réalisation de la prestation.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur les unités d'œuvres (UO) selon la table des profils et rappelant obligatoirement les travaux à réaliser, l'équipe et les livrables figurant au présent CCTP et le calendrier de réalisation.

Préalablement à toute intervention, le titulaire présentera à l'administration le profil et le CV de son intervenant pour validation.

Pour chaque commande de prestations exécutées hors Île de France, le titulaire ajoute dans son devis le surcoût prévu pour le déplacement (prix 6.3 de l'annexe financière) et éventuellement le surcoût correspondant à l'hébergement et la restauration correspondant à la durée d'exécution (prix 6.4 de l'annexe financière).

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.10 PRESTATION L3P7 - CONCEPTION ET DEVELOPPEMENT DE NOUVELLES FONCTIONNALITES BIOMETRIQUES (HORS ROADMAP EDETEUR) POUR L'ENSEMBLE DES PRODUITS BIOMETRIQUES DU LOT 3

OBJECTIFS DE LA PRESTATION

Cette prestation de conception et de développement consiste à créer de nouvelles fonctionnalités pour l'ensemble des produits du lot 3 non prévues initialement dans la feuille de route de l'éditeur ou réaliser des évolutions sur les composants biométriques objets du présent lot 3.

Le développement se fait selon les prescriptions de l'administration dans la feuille de route du CBIMI.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Au titre de cette prestation, il est attendu du titulaire au minimum les actions suivantes :

- Une analyse d'impact sur le ou les composant(s) concerné(s) ;
- La conception technique détaillée de la fonctionnalité.

Le titulaire réalise les développements et tests permettant de garantir la conformité, et qualité de la

fonctionnalité au besoin.

A ce titre il :

- développe les fonctionnalités complémentaires assortis de la typologie de tests réalisés et des tests de qualification et de non régression, gérés en configuration ;
- réalise et/ou maintient les scripts et outils permettant de réaliser les tests de charge et de performance ;
- met à jour l'ensemble de la documentation ;
- établit la fiche de livraison récapitulant le détail de la livraison .

À la demande de l'administration un support pourra être apporté concernant les déploiements applicatifs sur les différents environnements.

Chaque développement s'accompagne également d'une période de garantie d'un an au minimum pendant laquelle le titulaire réalise sans surcoût tout correctif de dysfonctionnement et le maintien en condition de sécurité du module ou de la fonctionnalité développée.

Il réalise ces correctifs et le maintien en condition de sécurité selon les mêmes principes que ceux mis en place pour la fourniture des composants tels que présentés dans les prestations précédentes.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit une expression de besoin de la fonctionnalité à développer avec le périmètre des composants ou modules concernés, complété d'un cas d'usage.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur les unités d'œuvres (UO) selon la table des profils et rappelant obligatoirement les travaux à réaliser, l'équipe et les livrables figurant au présent CCTP et le calendrier de réalisation.

Préalablement à toute intervention, le titulaire présentera à l'administration le profil et le CV de son intervenant pour validation.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

IX.11 PRESTATION L3P8 – FOURNITURE DE DONGLES GARANTIE STANDARD INCLUDE

OBJECTIFS DE LA PRESTATION

Cette prestation (PSE) a pour objet de permettre à l'administration d'acquérir des dongles de manière unitaire ou groupée en cas de perte, vol ou de détérioration dans l'hypothèse où le/ les produits biométriques du lot 3 sont déployés via cette configuration.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Le titulaire fournit le dongle en y associant le middleware précédemment acquis par l'administration.

Au titre de la garantie incluse, titulaire est l'interlocuteur unique et exclusif des services de l'administration. Il est seul responsable de la parfaite conformité des prestations attachées à la garantie pendant l'intégralité de leur période d'exécution. Par conséquent, il est interdit au titulaire d'orienter l'administration vers un constructeur, un sous-traitant ou un tiers mainteneur.

La garantie comprend : le dépannage par réparation ou remplacement des pièces ou sous-ensembles défectueux, usés ou cassés à la suite de l'usage conforme à la notice d'utilisation du matériel.

Sont exclus du service de garantie :

- ☐ la réparation des dommages ou défaillances du matériel résultant d'accidents ou de négligences non imputables au titulaire ou de l'accès frauduleux au matériel ;
- ☐ les conséquences de l'inobservation des conditions d'installation, d'environnement et d'utilisation ou des règles d'emploi du matériel ou de l'usage de courant électrique ou de fournitures ou de supports informatiques ne correspondant pas aux normes prescrites par le titulaire ;
- ☐ les extensions, connexions ou déconnexions non expressément prévues par le titulaire comme étant incluses dans le service ;
- ☐ la modification des matériels ou dispositifs à la demande de l'administration sauf orsque ces modifications ont été réalisées par le titulaire.

A compter de la saisine du titulaire par l'administration celui-ci dispose d'un délai maximal de soixante (60) minutes pour confirmer la demande à l'administration. Cette confirmation revêt la forme d'un courriel adressé au service demandeur. S'agissant de la garantie standard et de l'extension de la garantie, le titulaire s'engage à une garantie de temps de rétablissement (GTR) fixée à dix (10) jours ouvrés maximum, retour dans les locaux de l'administration inclus, à compter de la demande d'intervention

PREREQUIS FOURNIS PAR L'ADMINISTRATION

Le périmètre de l'intervention, ainsi que sa durée, seront précisés par l'administration, lors de la commande.

TYPE DE PRIX

Cette prestation est déclenchée par l'émission d'un bon de commande auprès du titulaire après établissement d'un devis basé sur un prix unitaire conformément à l'annexe financière.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version validée par ses équipes.

IX.12 PRESTATION L3P9 - REVERSIBILITE

OBJECTIFS DE LA PRESTATION

La réversibilité (ou transférabilité) a pour but d'organiser à l'issue de l'accord-cadre et sur le périmètre des développements spécifiques pour le ministère, un transfert de connaissances du titulaire à l'administration ou au bénéfice de toute autre personne désignée par l'administration ou de tout tiers désigné par celle-ci.

La réversibilité/transférabilité ne s'applique pas aux produits standards du titulaire mais seulement aux produits ou fonctionnalités développés et propriété de l'administration.

DEFINITION DES ACTIVITES ET DES TACHES A REALISER

Le titulaire assure, sur demande de l'administration et dans le délai imparti, une totale réversibilité/transférabilité des prestations de MCO/MCS et intégration des composants. Il s'interdit de faire obstacle à cette décision et s'engage à apporter toute l'assistance nécessaire à la bonne réalisation de cette opération tout en assurant la continuité de service.

La réversibilité/ transférabilité intervient soit dans le cas de la résiliation de l'accord-cadre soit à l'échéance de l'accord-cadre.

A ce titre, le titulaire :

- établit un plan de réversibilité/ transférabilité dans lequel il précise :
 - les rôles et responsabilités des interlocuteurs de l'administration du titulaire et du reprenant ;
 - les modalités de pilotage et de gestion des activités nécessaires au transfert de connaissance entre les acteurs ;
 - l'ensemble des éléments transférés dans leur dernière version (documents de conception, de réalisation d'installation, état des anomalies, etc.) ;
 - le planning de mise en œuvre de la réversibilité/ transférabilité ;
- assure le transfert de connaissances permettant à l'équipe du reprenant ou à l'administration de disposer de tous les éléments nécessaires à la reprise du périmètre ;
- forme l'équipe du reprenant ;
- assiste le reprenant ou l'administration lors de l'exécution de la reprise d'activité ;
- réalise le bilan de la réversibilité/transférabilité.

La réversibilité ou la transférabilité se déroule dans les locaux de l'administration.

Le titulaire nomme un responsable de la réversibilité/ transférabilité. Ce responsable est l'interlocuteur privilégié de l'administration, ou de ses représentants pendant cette période.

PREREQUIS FOURNIS PAR L'ADMINISTRATION

L'administration fournit :

- La date de début de la phase de réversibilité et le déclenchement de la prestation correspondante ;
- La désignation du Chef de Projet en charge pour l'administration du bon déroulement et du suivi de la réversibilité ;
- La composition de l'équipe du nouvel entrant, et la désignation de son responsable.

TYPE DE PRIX

La prestation de réversibilité est une prestation forfaitaire dont la durée est de deux (2) mois.

LIVRABLES

La liste des livrables ainsi que les délais de livraison et de vérification se trouve en annexe I du présent CCTP, dans le document intitulé « découpage des prestations et des livrables » (DPL). Le titulaire fournit à l'administration les livrables identifiés pour chaque prestation, dans une version stable.

