Voici une fiche de synthèse au format PDF. Elle est conçue pour être votre "document fondateur" : un cahier des charges minimaliste mais complet, servant de référence constante pour garder le cap, prendre des décisions cohérentes et suivre l'avancement.

# Fiche de Synthèse Projet : Plateforme d'Agents IA "Caméléon"

Version : 1.1

Date : 16 septembre 2025

Statut : Document de Cadrage Initial

## 1. Vision du Projet

Créer une plateforme SaaS (**S**oftware **a**s **a** **S**ervice) permettant aux PME et ETI de déployer rapidement des agents d'intelligence artificielle sur-mesure, adaptés à leurs processus métiers spécifiques. Le système est conçu comme un "caméléon" : un socle technique commun sur lequel se branchent des capacités modulaires pour répondre à des besoins précis sans réinventer la roue.

Le but ultime est de permettre aux utilisateurs de construire et d'opérer de véritables systèmes d'agents autonomes qui combinent ces capacités pour automatiser des processus complexes de bout en bout.

## 2. Objectif Principal (La "Mission")

**Démocratiser l'IA opérationnelle en la rendant agile, transparente et mesurable.**

Nous ne vendons pas de l'IA, nous vendons des résultats métiers quantifiables (temps gagné, réduction d'erreurs, conformité assurée) en fournissant des solutions packagées pour des niches spécifiques (Tourisme, Conformité, Fiscalité...) tout en construisant une plateforme robuste et ouverte.

## 3. Principe de Fonctionnement

La plateforme fonctionne sur un modèle "Cœur + Capacités" :

1. **L’Agent Orchestrateur (Le « Cerveau ») :** C’est le chef d'orchestre intelligent de la plateforme. Il lit les "recettes" de l'utilisateur et utilise les "packs" de capacités disponibles pour accomplir la mission de manière autonome. Il réside au sein du Cœur de la plateforme.
2. **Le Cœur (Core) :** Le socle technique qui héberge l'agent et fournit les services transverses essentiels (sécurité, multi-tenancy, logging...).

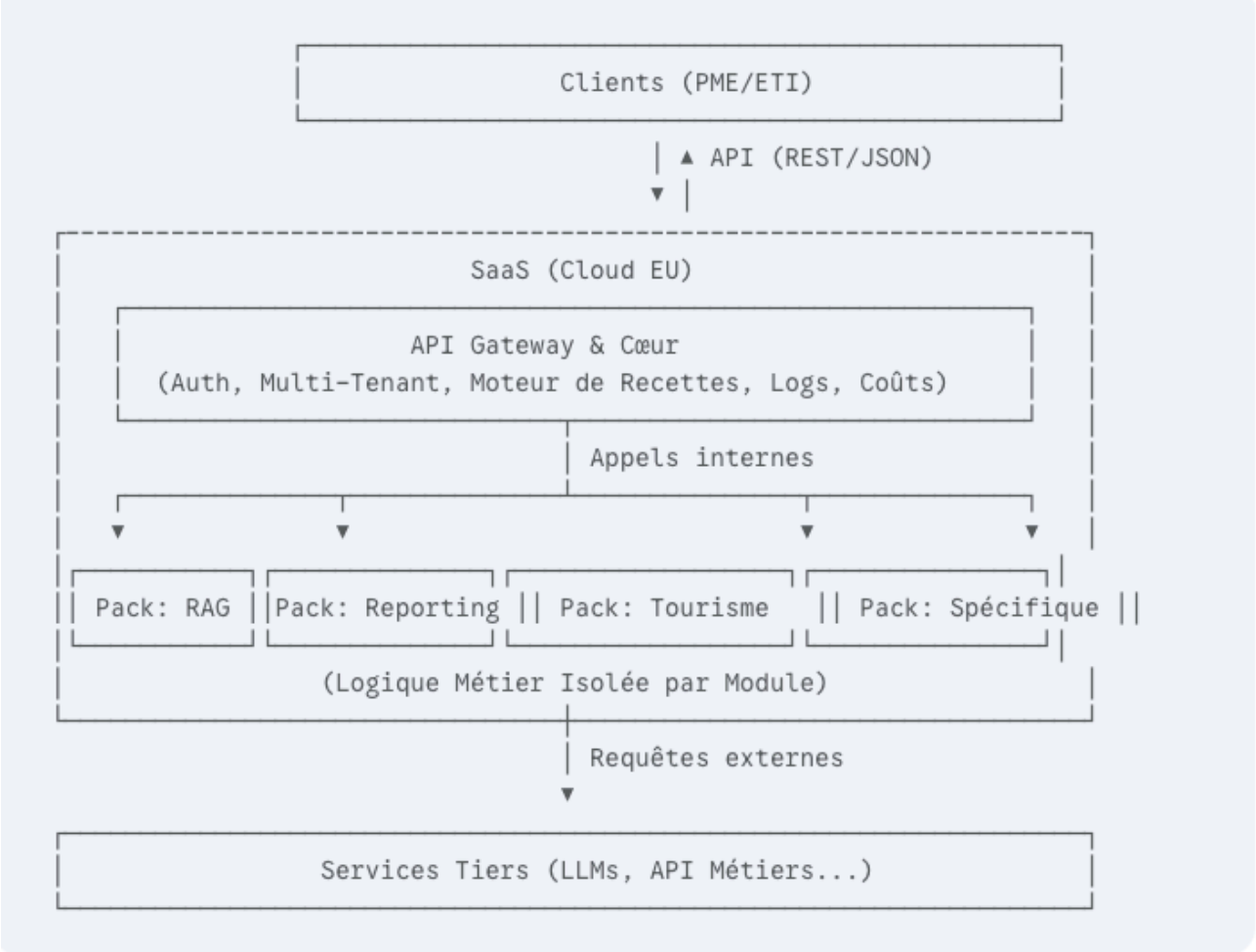
3. **Les Packs de Capacités :** Ce sont des briques logicielle indépendantes et réutilisables, chacune spécialisée dans une tâche (ex: Recherche Documentaire, Rédaction de Rapport, Connexion à une API métier).

4. **Les Recettes :** Ce sont les instructions en langage naturel ou scriptées que l'utilisateur fournit à l'Agent Orchestrateur pour qu'il exécute une tâche multi-étapes. (ex: "1. Chercher des informations dans le BOFiP. 2. Rédiger une synthèse.").

5. **Le Client (Tenant) :** Chaque entreprise cliente active les packs de capacités dont elle a besoin et utilise les recettes associées pour automatiser ses tâches.

## 4. Architecture de Référence (MVP)

L'architecture initiale est un **monolithe modulaire** : une seule application conçue pour être facile à déployer et à maintenir, mais structurée en interne pour pouvoir évoluer vers des microservices.



- **Base de données :** Une seule base **PostgreSQL** avec un schéma core pour les données communes et un schéma par capacité (rag, tourism...) pour isoler les données métiers.
- À long terme, une couche d'orchestration (l'Agent) viendra se placer au sein du "Cœur" pour piloter les "Appels internes" vers les différents packs de manière intelligente, en se basant sur les instructions des recettes.

## 5. Impératifs du Projet (Les "Règles d'Or")

- **Simplicité avant tout :** Toujours choisir la solution technique la plus simple qui répond au besoin. Pas de sur-ingénierie. On ajoute la complexité (ex: workflows asynchrones, microservices) seulement quand c'est indispensable.
- **Transparence radicale :** Le client doit avoir une visibilité claire sur les coûts (notamment les appels aux modèles de langage), la performance et les sources des informations générées.
- **Sécurité et Conformité dès le premier jour :**
  - **Isolation stricte des données clients (multi-tenancy).**
  - **Hébergement en Union Européenne.**
  - **Respect des principes du RGPD et anticipation de l'AI Act** (traçabilité, information de l'utilisateur).
- **Mesurer pour piloter :** Chaque fonctionnalité doit être associée à une métrique de succès (KPI) claire pour évaluer sa valeur et guider les développements futurs (ex: ROI client, taux d'adoption, qualité des réponses).
- **Focus sur le résultat métier :** La technologie est un moyen. Le succès du projet se mesure à la valeur apportée aux processus métiers du client.

## 6. La Modularité comme ADN

La modularité est le principe fondateur du projet. Elle garantit l'agilité et la pérennité de la plateforme.

- **Indépendance des Packs :** Chaque "pack de capacité" est développé et peut être mis à jour indépendamment des autres. Il expose ses fonctionnalités via une interface interne claire.
- **Réutilisabilité :** Une capacité générique (ex: Rédaction de Rapport) est développée une seule fois et réutilisée dans de multiples solutions métiers pour différents clients.

- **Évolution maîtrisée :** L'ajout d'une nouvelle fonctionnalité se traduit par la création d'un nouveau pack, sans impacter l'existant. Cela minimise les risques de régression.
- **Préparation pour l'avenir :** Cette structure modulaire est la base d'un véritable écosystème. En intégrant des protocoles ouverts comme le MCP, nous permettrons à l'**Agent Orchestrateur** de découvrir et d'utiliser dynamiquement une infinité d'outils (packs). La plateforme évoluera ainsi d'une suite d'outils puissants à un **véritable système d'exploitation pour agents autonomes**, capable d'automatiser des processus bien au-delà du simple RAG.