

Mon Compte Mobilité

**Document d'Architecture Technique
Version 1.1**

Sommaire

1. Introduction	5
1.1. Définitions	5
1.2. Documents de référence	6
1.3. Documents applicables	6
1.4. Table des révisions	6
2. Contexte et motivation du projet	7
2.1. Ecosystème	7
2.2. Positionnement	8
2.3. Objectifs.....	12
2.4. Hors scope du PMV	12
2.5. Contraintes	12
2.6. Périmètre du DAT	13
3. Architecture conceptuelle.....	14
3.1. Hypothèses fonctionnelles.....	14
3.2. Acteurs	14
3.3. Processus métier	17
3.4. Cas d'utilisation	21
3.5. Cartographie fonctionnelle	29
3.6. Principaux concepts métier	30
3.7. Exigences fonctionnelles	37
3.8. Exigences non fonctionnelles.....	41
4. Architecture logique	45
4.1. Architecture Hub	45
4.2. Sous-systèmes et dépendances	46
4.3. Stockage et utilisation des données	47
4.4. Flux et cinématique.....	48
5. Principes directeurs.....	53
6. Architecture technique	55
6.1. Schéma de principe	55
6.2. Justification des choix d'architecture	57
6.3. Architecture technique du PMV	57
6.4. Licences open sources autorisées.....	58
6.5. Composants logiciels.....	60
6.6. Provisionnement des ressources dans Azure.....	62
6.7. Schéma réseau.....	63
6.8. Plateformes et environnements	65
7. Sécurité	67
7.1. Gestion des identités, identification & authentification	67
7.2. Certificats serveurs et nom de domaine	68
7.3. Autorisation et contrôle d'accès	68

7.4. Intégrité	68
7.5. Confidentialité	68
7.6. Traçabilité / Journalisation	69
7.7. Imputabilité et non répudiation	69
7.8. Anonymisation & Pseudonymisation des données.....	69
7.9. GDPR	69
7.10. Sauvegarde / restauration	70
7.11. Purge	70
7.12. Archivage	70
7.13. Anti-virus / anti-malware.....	70
7.14. Tests d'intrusion / Revues de Code Source.....	71
7.15. Limitation volumétrie	71
7.16. Anti-DDoS	72
7.17. Cloisonnement	72
7.18. Système de détection d'intrusion	72
7.19. Montée de version des systèmes d'exploitation et patchs sécurité	72
8. Modèle de dimensionnement théorique.....	73
8.1. Entrants du GART	73
8.2. Hypothèses de Capgemini.....	73
8.3. Modèle de dimensionnement théorique.....	74
9. Processus de livraison	75
9.1. Préparation et définition des jobs de livraison.....	75
9.2. Livrables.....	79
10. Approche DevOps	81
10.1. Introduction à GitOps	81
10.2. Implémentation	82
10.3. Pipelines de build et déploiement	84

Tables des illustrations

Figure 1 – Rôles dans l'écosystème des MaaS	7
Figure 2 – Rôles et services dans l'écosystème des MaaS	8
Figure 3 - Enjeux de la Standardisation des MaaS	9
Figure 4 - Apports de la Standardisation des MaaS	10
Figure 5 - Cas d'utilisation	23
Figure 6 - Point de vue du visiteur	24
Figure 7 - Point de vue du citoyen	24
Figure 8 - Point de vue du financeur	25
Figure 9 - Point de vue de l'administrateur fonctionnel	25
Figure 10 - Point de vue de l'administrateur technique	26
Figure 11 – Cartographie fonctionnelle	29
Figure 12 – Principaux concepts métiers	31
Figure 13 – Architecture générale	45
Figure 14 – HUB locaux	46
Figure 15 – Sous-systèmes logiques	47
Figure 16 – Flux et cinématique – vue d'ensemble	48
Figure 17 – Principe de l'habilitation FranceConnect	50
Figure 18 – Authentification via FranceConnect	51
Figure 19 – API FranceConnectées	52
Figure 20 – Principes directeurs d'architecture	53
Figure 21 – Architecture technique – schéma de principe	55
Figure 22 – Architecture technique – Solution retenue/enrichie pour le PMV	58
Figure 23 – Options de segmentation du trafic réseau dans Azure	63
Figure 24 – Options de segmentation du trafic réseau dans Azure	64
Figure 25 – Organisation des ressources dans Azure	65
Figure 26 – Fonctionnement de l'Antivirus ClamAV	71
Figure 27 – Principes de GitOps	82
Figure 28 – Approche DevOps : orientation GitOps	83

1. Introduction

Ce document présente l'architecture du système Mon Compte Mobilité « moB » et son extension (CME) dans son écosystème.

1.1. Définitions

Terme	Description
MSP	“Mobility Service Provider”, fournisseur d'un service de mobilité.
MaaS	“Mobility As A Service”, plateforme réunissant l'information, la réservation et le paiement de l'ensemble de l'offre de mobilité disponible.
MCM	Mon Compte Mobilité
moB	Appellation produit du projet Mon Compte Mobilité
Std MaaS	Standardisation des MaaS
Gateway (GW)	Passerelle de gestion des échanges entre les MaaS et les MSP
CME	Compte Mobilité Etendu
CMS	Compte Mobilité Standardisé
HUB	Plateforme regroupant les services MCM de Compte Mobilité (MOB / CME) et de Gateway
Mobilité durable	Mobilité décarbonnée.
RGPD	Règlement Général sur la Protection des Données.
RGAA	Référentiel Général d'Accessibilité pour les Administrations.
CNIL	Commission Nationale de l'Informatique et des Libertés
CEE	Certificats d'Économie d'Energie
SIS	Système d'Information et de Services pour la billettique
SIV	Système d'Information Voyageur
TC	Transports en Commun
IV	Information Voyageur
RI	Recherche d'Itinéraires
IVTR	Information Voyageur Temps Réel
REF	Référentiel
IDFM	Île-de-France Mobilités
M2A	Mulhouse Alsace Agglomération
GART	Groupement des Autorités Responsables de Transport
AOM	Autorité Organisatrice de Mobilité
PRIM	Plateforme Régionale d'Information pour la Mobilité
VE	Véhicule Électrique
VLS	Vélo en Libre-Service

VTC	Véhicule de Tourisme avec Chauffeur
PMV	Produit Minimum Viable (MVP Minimum Viable Product)
CSP	Cloud Service Provider
SAST	Static Application Security Testing

1.2. Documents de référence

N°	Document	Version	Date
[R03]	Référentiel général d'amélioration de l'accessibilité	4.0	Août 2019
[R04]	MCM – Hypothèses-PMV1	V0.3	14 Sept 2020
[R05]	MCM_Référentiel données et traitements	v1	20 Juil 2020

1.3. Documents applicables

N°	Document	Version	Date
[A01]	fabmob/CMS: Compte Mobilité Standardisé (github.com)		01/09/2022

1.4. Table des révisions

N°	Document	Version	Date
	WIP-DAT-v0.6.docx	0.4	09/2020
	DAT-v1.0.docx	1.0	09/2022
	DAT-MCM_moB_V1.1.docx	1.1	11/2022

2. Contexte et motivation du projet

2.1. Ecosystème

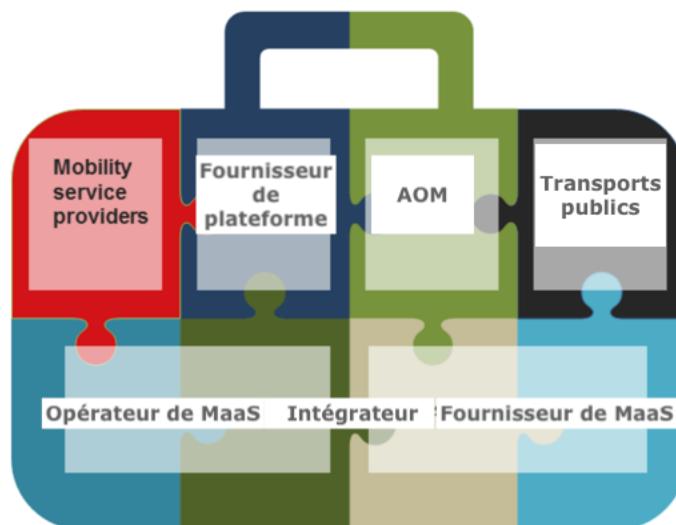


Figure 1 – Rôles dans l'écosystème des MaaS

Source : <https://www.transport20.no/wp-content/uploads/2016/06/maas.pdf>

Le projet Mon Compte Mobilité s'inscrit dans l'écosystème de la mobilité et des MaaS. Ce dernier est l'objet de nombreuses publications qui introduisent une nomenclature des rôles joués par les différents acteurs :

- Les fournisseurs de MaaS qui éditent des frameworks ou des solutions logicielles clé en main permettant de mettre en œuvre des MaaS ;
- Les intégrateurs qui prennent en charge le déploiement, la configuration, l'interconnexion et l'extension éventuelle des systèmes de MaaS ;
- Les opérateurs sont responsables du fonctionnement, de la sécurisation, de la surveillance, du maintien en condition opérationnelle et du support aux usagers ;
- Les Mobility Service Providers (MSP) fournissent des services de mobilité qui sont agrégés par les MaaS ;
- Ils s'appuient sur des services d'infrastructure ou de plateforme fournis par des tiers (fournisseurs de plateforme) ;
- Les AOM (Autorité Organisatrice de la Mobilité) assurent l'organisation du réseau de transport urbain sur leurs territoires. Elles en délèguent le plus souvent l'exploitation à des tiers.

Certains acteurs peuvent porter plusieurs de ces rôles simultanément.

Selon ces définitions, Mon Compte Mobilité serait :

- Une plateforme ;
- Au service des AOM, des collectivités et entreprises et des citoyens ;
- S'appuyant sur des MaaS et MSP ;
- S'appuyant sur d'autres plateformes techniques comme FranceConnect ou Azure ;
- Développée conjointement par Capgemini et la Fabrique des Mobilités ;
- Opérée dans un premier temps par Capgemini puis transmis à un tiers non identifié à ce stade.

2.2. Positionnement

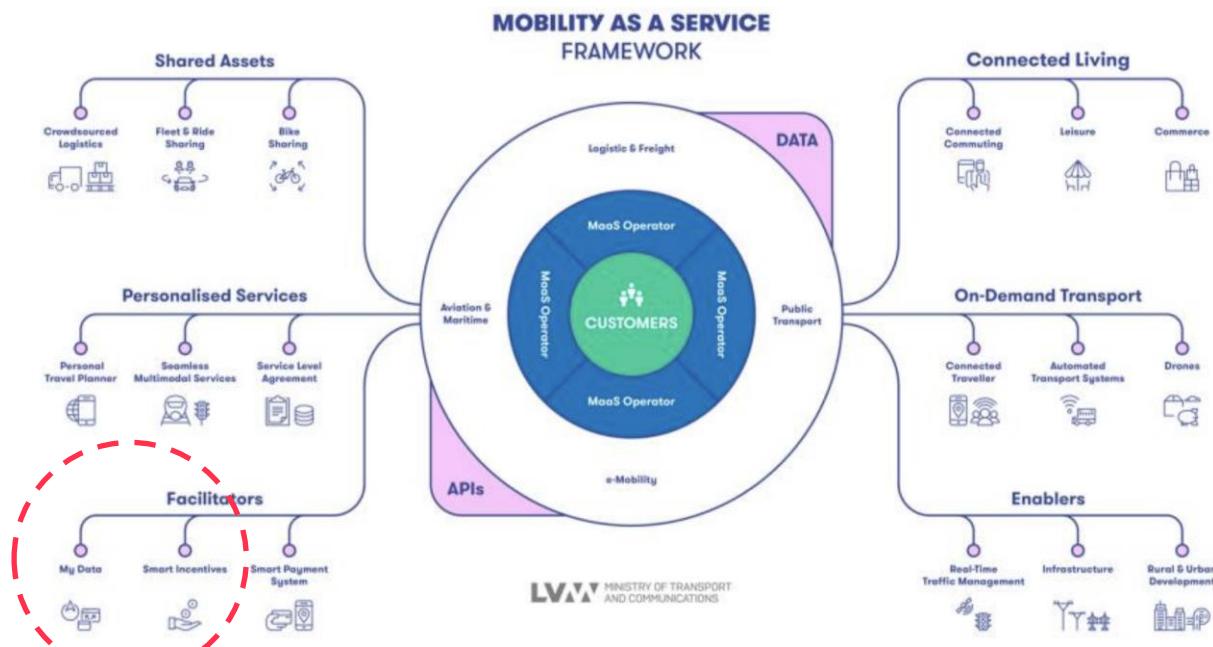


Figure 2 – Rôles et services dans l'écosystème des MaaS

Source : <https://maas-alliance.eu/wp-content/uploads/sites/7/2018/09/Vision-Paper-on-Multimodal-Passenger-rights-240918-FINAL.pdf>

Le schéma ci-dessus illustre les services pouvant être offerts par ou construits autour des MaaS.

Le positionnement de Mon Compte Mobilité consiste à promouvoir l'usage de moyens de mobilité douce en rendant plus accessibles aux citoyens les offres de mobilité et les dispositifs incitatifs correspondants proposés par les organismes publics et les entreprises. Mon Compte Mobilité doit également fournir de la donnée agrégée à ces mêmes acteurs afin de les aider à piloter leurs offres, leurs financements et optimiser la mobilité sur leurs territoires.

Mon Compte Mobilité ne doit pas entrer en compétition ou empiéter sur les domaines des autres acteurs privés. Il ne doit pas par exemple devenir un super-MaaS ou remplacer les supports de paiement.

2.2.1. Extension de Mon Compte Mobilité

Ce projet élargit grandement la visée du projet Mon Compte Mobilité.

Les travaux du projet initial MCM donnent lieu au développement et au déploiement du produit « moB » se voulant innovant mais restant spécifique à un besoin, celui de la gestion des aides à la mobilité durable et douce.

Ce besoin s'inscrit dans un contexte d'écosystème très riche et complexe, entre des collectivités (AOMs), des entreprises et des acteurs de la mobilité tels que les MaaS.

Au sein d'un tel écosystème, de nombreux enjeux de standardisation existent depuis plusieurs années et prennent de plus en plus d'importance. Parmi ces enjeux, beaucoup sont liées aux MaaS et moB est donc directement concerné.

C'est pourquoi les travaux sur le programme MCM ont été étendus avec un projet avenant au programme MCM appelé « Standardisation des MaaS ».

2.2.2. Enjeux de standardisation

Cette extension de projet vise donc à répondre à certains enjeux de standardisation, illustrés et définis ci-après.



Figure 3 - Enjeux de la Standardisation des MaaS

Pour chacun des acteurs principaux de l'écosystème présenté en amont, le projet permettra de répondre aux à leurs différents enjeux :

- **MaaS**
 - o Réduire les coûts de développement et de maintien des interfaces spécifiques avec les MSP
 - o Faciliter leur construction
 - o Faciliter l'intégration des MSP & comptes mobilité dans les MaaS pour limiter les coûts
- **MSP**
 - o Réduire la redondance et la complexité d'intégration à des plateformes de mobilité
 - o Réduire les coûts d'interfaces pour les MSP
 - o Augmenter les perspectives de croissance des MSP, notamment les petits acteurs locaux, en leur facilitant l'accès aux citoyens
- **AOM**
 - o Développer l'offre de mobilité du territoire et renforcer son attractivité
 - o Changer les comportements grâce à une mobilité plus fluide
 - o Permettre l'émergence de nouveaux acteurs engagés pour la transition énergétique
 - o Abaisser la barrière financière et technique à l'entrée pour développer des MaaS
 - o Favoriser l'harmonisation de la mobilité et faciliter la synchronisation des travaux entre les AOMs
- **Citoyen**

- Réduire la dispersion des offres de mobilité sur les territoires en augmentant la multimodalité et la portée géographique
- Faciliter l'usage de la mobilité servicielle en simplifiant et en unifiant les parcours : expérience utilisateur sans couture

La standardisation permettra de relier plusieurs MSP à un ou plusieurs MaaS via des interfaces standards ainsi que de faciliter l'intégration des MSP et de MOB / CMS dans les MaaS

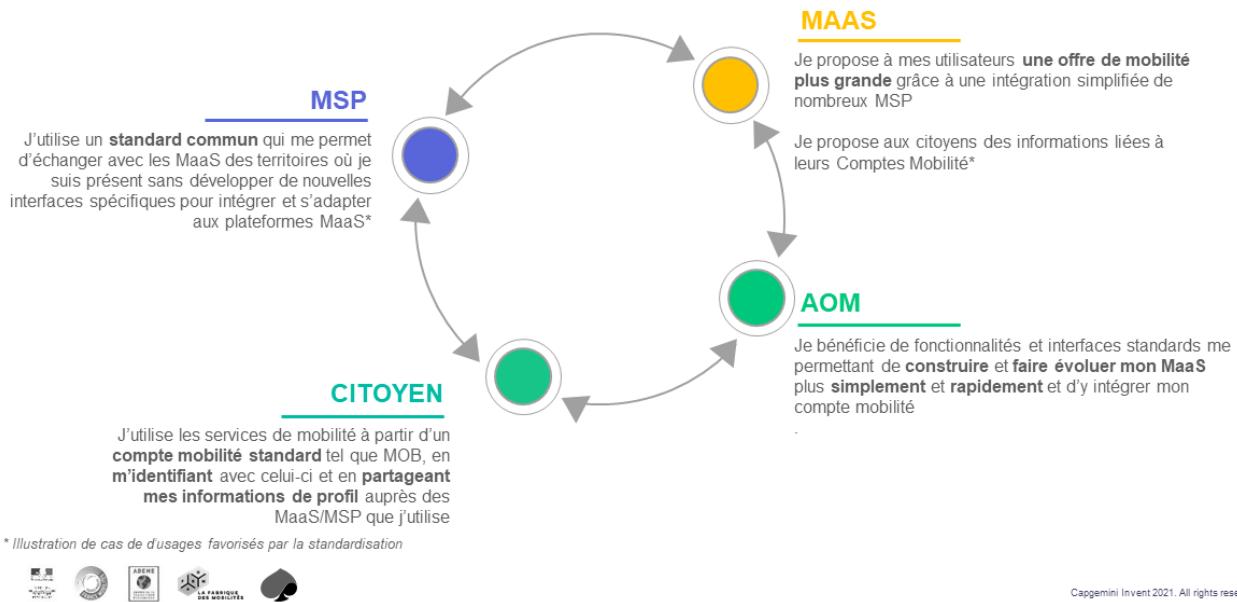


Figure 4 - Apports de la Standardisation des MaaS

Compte Mobilité Standardisé

Tout opérateur de mobilité et opérateur de MaaS gère des comptes utilisateurs indispensables au fonctionnement des services proposés. Dans ce contexte chacun de ces comptes utilisateur constitue un "compte mobilité" puisqu'il contient des données personnelles génériques, des données de profil propres au contexte mobilité (préférences de déplacement, abonnements, droits d'accès, caractéristiques de déplacement et de véhicules par exemple) et éventuellement des données d'usage des services et/ou de déplacement de l'utilisateur.

Dans le cadre de systèmes "Mobility as a Service" plusieurs comptes mobilité qui concernent le même usager final interagissent. Plusieurs fonctionnalités clef attendues ont d'ores et déjà été identifiées, pour lesquels une standardisation des méthodes ou des pratiques de mise en œuvre est requise. Sont citées ici 9 fonctionnalités clef identifiées dans le cadre des travaux du GART, qui devront être complétées et approfondies au cours du processus d'élaboration du standard.

- CM01 - Créer, modifier ou supprimer un compte mobilité
- CM02 - Permettre la connexion à un compte mobilité et l'authentification unique
- CM03 - Gérer et accéder aux informations du compte
- CM04 - Créer (enrôlement) et modifier un compte chez un partenaire
- CM05 - S'assurer de la protection des données personnelles
- CM06 - Gérer les préférences de voyage

- CM07 - Contrôler les comptes frauduleux
- CM08 - Permettre le lien des comptes porteur / payeur
- CM09 - Recueillir et traiter les pièces justificatives

Pour rendre disponibles de manière standardisée ces différentes fonctionnalités, les travaux de standardisation du Groupe de Travail “Compte Mobilité Standardisé” pourront notamment standardiser :

- La description des informations présentes ou disponibles dans un “Compte Mobilité”, leur représentation technique, ainsi que la qualification de leur source ou de leur qualité ;
- La gestion des consentements et des droits associés, pour chaque utilisateur et chaque contexte ;
- Des interfaces pour la création de compte à partir d'un autre compte mobilité standardisé, l'appariement de comptes existants, l'échange de données standards entre ces comptes, ainsi que l'échange de justificatifs ou preuves de validation ;
- Le choix des standards pour le SSO et la manière de les configurer, afin que différents systèmes les mettent en œuvre de manière similaire, ce qui réduira la complexité technique et ouvrira la voie à des comptes unifiés territoriaux ou nationaux à moindres frais.

Le standard est référé sous les termes “Compte Mobilité Standardisé” ou “CMS” et fera l'objet d'adaptations dans d'autres langues dont l'anglais.

Mon Compte Mobilité (moB) est de facto un candidat privilégié pour **adopter et soutenir le CMS** au sein de l'écosystème des comptes mobilité. En effet, sur la base de ce **compte unique**, les autres comptes adoptant le CMS pourraient **accéder aux informations de ce compte via ce standard**, après **consentement** du **citoyen** pour faciliter l'accès à d'autres services.

2.2.3. Hub Mon Compte Mobilité

Le programme Mon Compte Mobilité devient alors un HUB concentrant les acteurs de la mobilité et plus particulièrement les MaaS et les MSP autour des grands éléments suivants :

- **MON COMPTE MOBILITE (moB)**, spécification et construction d'un compte mobilité partagé et utilisable par tous, compte mobilité unique de gestion et d'accès aux aides à la mobilité, sera un démonstrateur de ce CMS
- La **GATEWAY**, passerelle d'accès standards aux services des MSPs

Le positionnement du HUB Mon Compte Mobilité consiste à promouvoir l'usage de moyens de mobilité douce en rendant plus accessibles aux citoyens les offres de mobilité et les dispositifs incitatifs correspondants proposés par les organismes publics et les entreprises, via un compte mobilité unique, s'appuyant sur l'identité FranceConnect.

Le HUB à l'aide de sa Gateway, doit fournir un point d'accès unique à ces mêmes acteurs afin de les aider à élargir leur offre, piloter leurs financements et optimiser la mobilité sur leurs territoires.

Il y a un unique HUB pour le PMV.

Ce HUB pourrait être décliné selon différentes instances à l'issue de la phase d'expérimentation, selon les stratégies de déploiement et les objectifs territoriaux qui seront poursuivis, notamment par le ou les futurs ré utilateurs du projet.

2.3. Objectifs

Les objectifs du PMV moB sont :

1. Inciter les citoyens à utiliser des moyens de mobilités durables.
2. Donner la visibilité sur l'offre existante des dispositifs d'aide à la mobilité du territoire.
3. Permettre aux citoyens de souscrire à un dispositif d'aide.
4. Permettre aux entreprises d'améliorer leur image de marque.
5. Faciliter la gestion des politiques de mobilité des entreprises.
6. Donner aux entreprises la visibilité sur l'utilisation des dispositifs d'aide proposés à leurs employés.
7. Faciliter la gestion du back office des collectivités.
8. Donner aux collectivités la visibilité sur l'utilisation des dispositifs d'aide proposés aux citoyens.

Les objectifs du PMV CME sont :

1. Permettre aux citoyens de s'authentifier avec FranceConnect
2. Permettre aux citoyens de certifier son identité avec FranceConnect
3. Inciter les MaaS/MSP à proposer l'authentification via moB (moB Connect)
4. Faciliter la souscription aux aides en intégrant les justificatifs fournis par les MaaS/MSP
5. Adopter la structure du Compte Mobilité Standardisé
6. Permettre aux citoyens de partager des informations sur ses préférences de mobilité
7. Permettre aux citoyens de partager des informations sur ses titres de transport (ex. permis de conduire)
8. Permettre aux citoyens de partager des informations obtenues via des API FranceConnectées (fiscales, étudiant, ...)

2.4. Hors scope du PMV

Les cas d'usage et fonctionnalités suivants ne sont PAS couverts par le PMV :

- Trajets multimodaux ;
- Interopérabilité entre les MaaS ; le HUB n'est pas un intermédiaire possible entre 2 solutions MaaS;
- Pas de paiement via moB ;
- Pas d'informations de géolocalisation stockées ;
- Les informations temps-réel des transporteurs ne transiteront pas par MCM.

Par ailleurs les limitations suivantes sont admises :

- Les usagers des MaaS et MSP seront redirigés vers moB selon le parcours choisi par le fournisseur de service. Les MSP et MaaS ne renverront programmatiquement à MCM aucune information de mobilité des usagers.

2.5. Contraintes

2.5.1. Existant des territoires

Le projet Mon Compte Mobilité aura à terme une portée nationale. Dans un premier temps, les territoires pilotes seront en nombre limité. Toutefois, il est probable que leurs maturités et leurs organisations diffèrent.

Dans tous les cas, Mon Compte Mobilité devra être en mesure de prendre en compte les choix déjà effectués par les régions et l'existant de la mobilité.

2.5.2. Existant des entreprises

De même, Mon Compte Mobilité prendra en compte la diversité des entreprises. Leur spectre s'étend des microentreprises/TPE peu équipées en infrastructures techniques, aux GE en passant par les PME et ETI plus matures. Il est possible qu'elles disposent déjà de solutions pour gérer les demandes de leurs collaborateurs voire d'un système ou d'un service dédié à la mobilité, d'un backoffice et de personnel dédié. Certaines auront déjà mis en place un service d'authentification. Plus rares seront celles en mesure de fournir des services programmatiques/APIs destinées à l'interfaçage avec Mon Compte Mobilité.

2.5.3. Protection des données

Le règlement n°2016/679, dit Règlement Général sur la Protection des Données (RGPD) doit être appliqué sur les données à caractère personnel.

2.5.4. Accessibilité

Le décret n° 2009-546 du 14 mai 2009 pris en application de l'article 47 de la loi n° 2005-102 du 11 février 2005 sur l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées et créant un référentiel d'accessibilité des services de communication publique en ligne, rend obligatoire l'accessibilité des services de communication publique en ligne aux personnes handicapées.

Malgré le fait que cette contrainte d'accessibilité ne s'applique pas dans la phase d'expérimentation de moB, le niveau recommandé d'accessibilité par l'Union européenne est le niveau double A (AA), ce qui correspond à la norme RGAA version 4.0 ([\[R03\]](#)).

Les interfaces web et mobile (web responsive) doivent satisfaire à ce niveau d'accessibilité.

2.6. Périmètre du DAT

L'architecture décrite dans ce document est relative au PMV et uniquement au produit moB, issu des travaux engagés par les projets MCM Historique et MCM Avenant partie CME.

Note importante : cette version n'inclut pas les évolutions fonctionnelles et techniques engagées dans le cadre des travaux avec les acteurs RPC et MSP covoiturage, visant à mettre en œuvre la mesure du Plan Sobriété du gouvernement d'Octobre 2022 sur l'incitation financière de 100€ pour le covoiturage.

En particulier, le dimensionnement est établi sur la base des objectifs de la première phase du projet.

3. Architecture conceptuelle

3.1. Hypothèses fonctionnelles

Les hypothèses fonctionnelles retenues sont en partie issues du document [[R04](#)].

- Le processus de création de compte citoyen prendra en compte l'apport de preuve pour son identité (via FranceConnect), son adresse et/ou sa commune de résidence (manuelle) et tout autre pièce justificative (par dépôt et validation manuelle)
- Le citoyen pourra justifier de sa commune par un dépôt de pièce justificative qui sera validé dans le backoffice moB (manuellement et non pas par une API externe de type [Justif'Adresse](#))
- Les entreprises et collectivités seront créés dans la plateforme via un backoffice accessible uniquement par les administrateurs moB
- Les offres de mobilité seront publiées uniquement par l'administrateur moB
- Les dispositifs d'incitations peuvent être publiés uniquement par l'administrateur moB
 - Les dispositifs seront transmis par un collaborateur d'une entreprise et/ou un employé d'une collectivité par un processus externe à la plateforme
- Le citoyen ne sera pas notifié automatiquement de la mise à disposition d'un nouveau dispositif d'incitation
- L'éligibilité du citoyen à une subvention proposée par moB ne sera pas calculée automatiquement en amont du processus de souscription
- Les demandes d'affiliation (d'un collaborateur à une entreprise) sont validées manuellement par l'entreprise
- Chaque entreprise aura au moins un collaborateur qui pourra valider les demandes d'affiliation et les demandes de dispositifs
 - Ces collaborateurs seront créés manuellement dans le backoffice moB uniquement par les administrateurs moB
- En PMV, le déclenchement du processus de règlement se réduira à la possibilité pour le financeur d'exporter (fichier structuré) l'ensemble des demandes de dispositifs validées pour intégration manuelle à son SI
- Les MAAS/MSP qui le souhaitent pourront proposer à leurs usagers de se connecter et/ou créer leurs comptes via moB (i.e. implémenter un bouton moB Connect sur leur page de connexion).
- Dans le cadre des obligations de la CNIL, l'utilisateur pourra télécharger ses données personnelles et demander la suppression de son compte

3.2. Acteurs

Le tableau ci-dessous présente les différents titres auxquels un utilisateur peut être amené à interagir avec Mon Compte Mobilité. Il existe une hiérarchie entre ces rôles.

Les acteurs et rôles abstraits apparaissent en italique.

Pour chaque catégorie, nous précisons si une interface homme-machine (IHM) est mise à disposition et si une authentification est requise.

Acteurs et rôles	Héritent de	IHM	Auth.	Description (PMV)
Visiteurs		Oui	Non	Les visiteurs sont les utilisateurs qui ne possèdent pas de compte dans moB ou qui

				ne se sont pas encore authentifiés. Ils n'ont accès qu'à un ensemble restreint de fonctionnalités telles que la consultation du contenu rédactionnel, des offres de mobilité, la création d'un profil, l'authentification et demander d'être informé de la disponibilité de moB dans sa région.
<i>Utilisateurs</i>		Oui	Oui	Lorsqu'un visiteur crée son compte, il devient un utilisateur de la plateforme. Une fois authentifié, il a accès à la gestion de son profil, à un tableau de bord, ainsi qu'à toutes les fonctionnalités libres/exposées aux visiteurs anonymes, et soumettre un ticket de support
Citoyens	Utilisateurs	Oui	Oui	Ils représentent l'une des catégories d'utilisateurs identifiés avec les financeurs et les administrateurs. Ils ont la possibilité de rejoindre des communautés (définies par des collectivités ou des employeurs), de soumettre des demandes d'aide à la mobilité, de suivre leur avancement et fournir des justificatifs le cas échéant. Ils peuvent aussi naviguer vers les sites des MaaS et MSP, en bénéficiant d'une authentification unique lorsqu'elle est configurée et supportée par la destination.
Financeurs	Utilisateurs	Oui	Oui	Ce sont les collectivités ou entreprises affiliées à moB. Via la plateforme, elles peuvent publier des aides à la mobilité, définir les communautés qui y ont accès, approuver les demandes de rattachement, instruire les demandes d'aide à la mobilité soumises par les usagers.
Administrateurs fonctionnels moB	Utilisateurs	Oui	Oui	Ils doivent pouvoir gérer le contenu rédactionnel du site Mon Compte Mobilité, déclarer les MaaS/MSP affiliés, leurs offres de mobilité ainsi que les aides à la mobilité non rattachées à des collectivités ou des entreprises spécifiques, et gérer les demandes de support. Il peut s'agir par exemple des droits salariés en général.
Administrateurs techniques moB	Utilisateurs	Oui/Non	Oui	Lors du rattachement d'un MaaS, d'un MSP, d'une collectivité ou d'une entreprise.

3.2.1. Liste des MaaS participants

Dans cette section, les acteurs MaaS participant au PMV seront listés au fur et à mesure ici. Le type d'intégration y sera précisé.

MaaS	AOM	Niveau d'intégration
IDFM	Île-de-France	Liaison de compte moB <u>existant</u> Affichage des aides via API moB Transmission des métadonnées de justificatifs d'achat sélectionnés par le citoyen Parcours de souscription en Webview moB Visualisation des souscriptions en webview moB
CMM	Mulhouse Alsace Agglomération	Lien vers création de compte de moB Liaison de compte moB existant Affichage des aides via API moB Parcours de souscription via API moB Visualisation des souscriptions via API moB
Mobil'Aude	Département de l'Aude	

3.2.2. Liste des Financeurs

3.2.2.1. Liste des Entreprises participantes

Dans cette section, les collectivités participant au PMV seront listés au fur et à mesure ici. Le mode d'affiliation des citoyens et l'interface de gestion des souscriptions à une aide y est précisé.

Entreprise	Territoire	Mode d'affiliation	Interface de gestion des souscriptions
Capgemini	Île-de-France	Approbation automatique via email professionnel	<u>MyConnect</u> (Neocase Software)
Capgemini	Mulhouse	Approbation automatique via email professionnel	<u>MyConnect</u> (Neocase Software)
FNOGEC	France	Approbation manuelle par un gestionnaire	moB
CAF du Haut-Rhin	Haut-Rhin	Approbation automatique via email professionnel	moB

--	--	--	--

3.2.2.2. Liste des Collectivités participantes

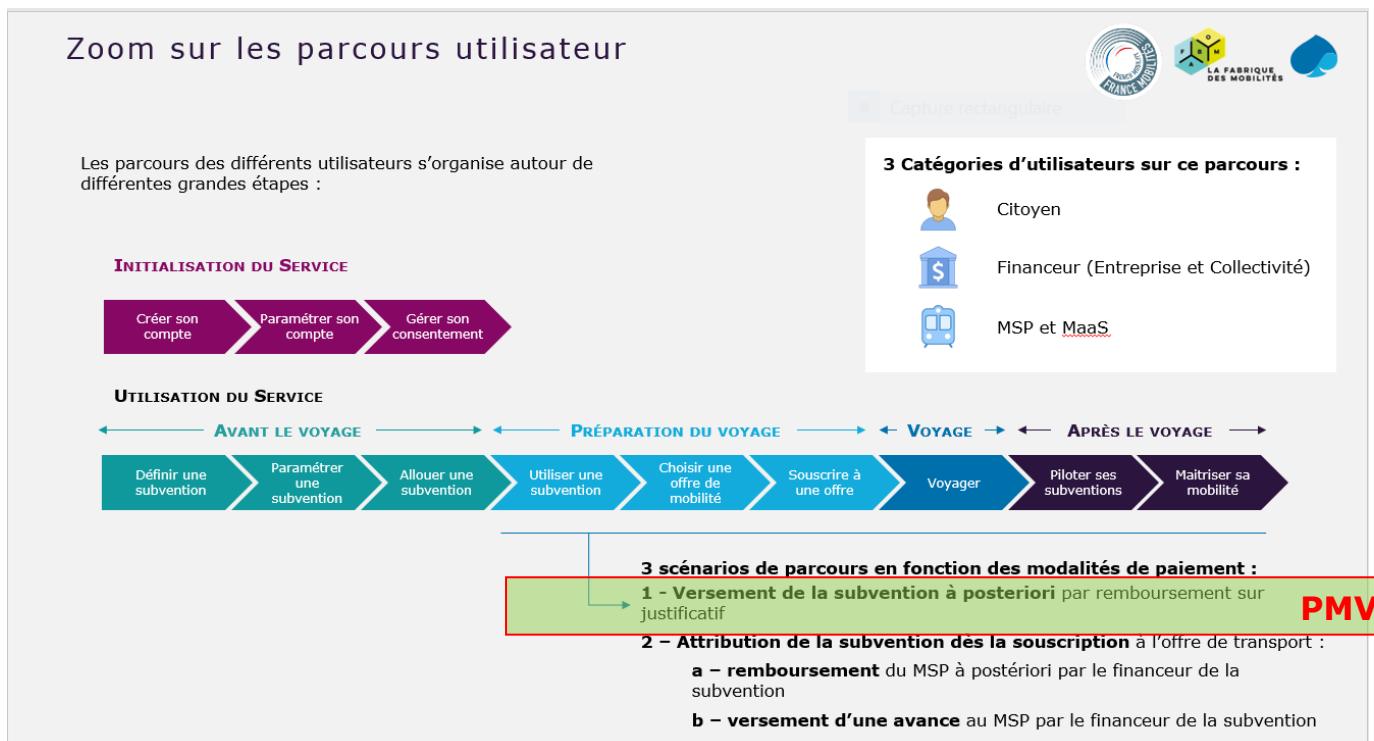
Dans cette section, les collectivités participantes au PMV seront listés au fur et à mesure ici. Le mode d'affiliation des citoyens y est précisé.

Collectivité	Territoire	Mode d'affiliation	Interface de gestion des souscriptions
	Île-de-France	N/A	Externe
	Grand-Est	N/A	Externe
	Occitanie	N/A	Externe

3.3. Processus métier

Dans les différents processus métiers ci-dessous sont encadrées en vert les activités concernant la solution MCM dans le PMV.

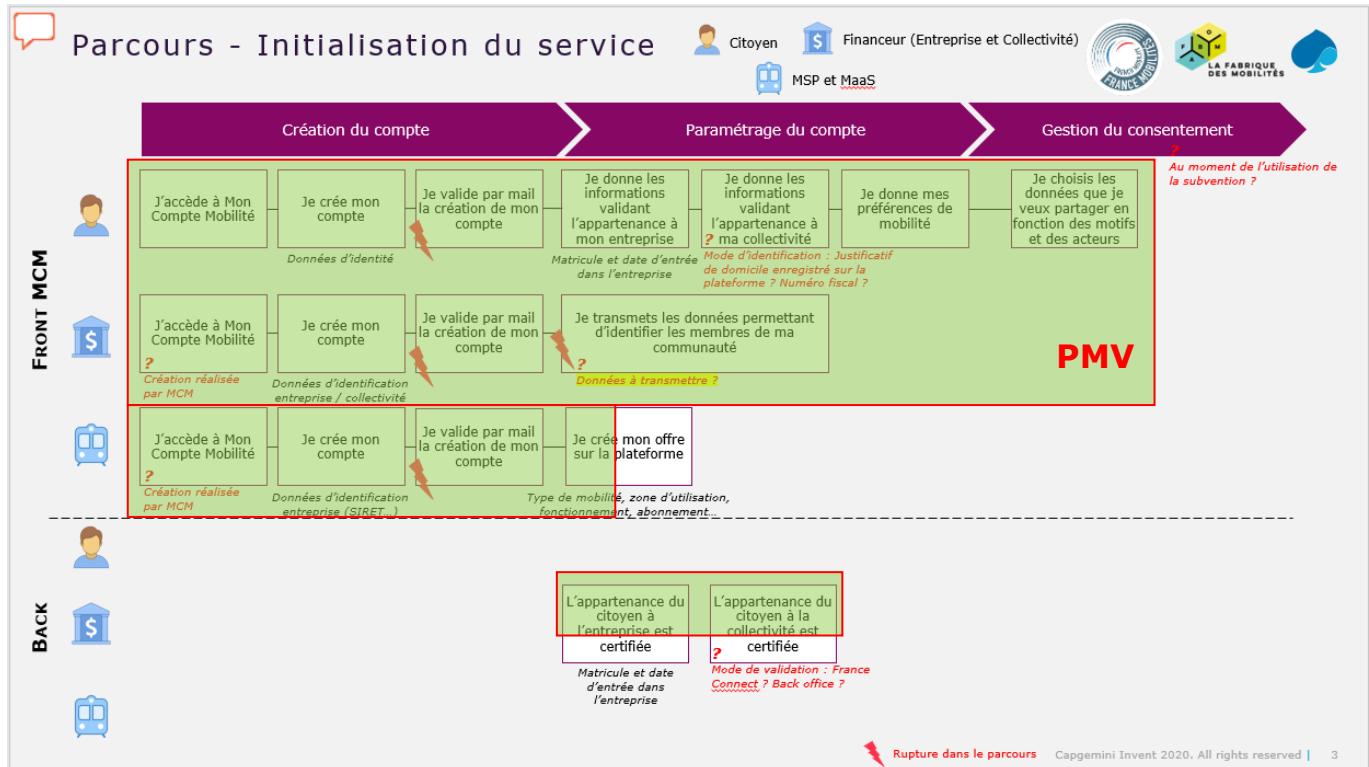
3.3.1. Processus complet



Précisions :

- Le versement de la subvention reste de la responsabilité du financeur et est réalisé à postérieur, après validation de la demande par ce dernier. moB ne gère pas le paiement.

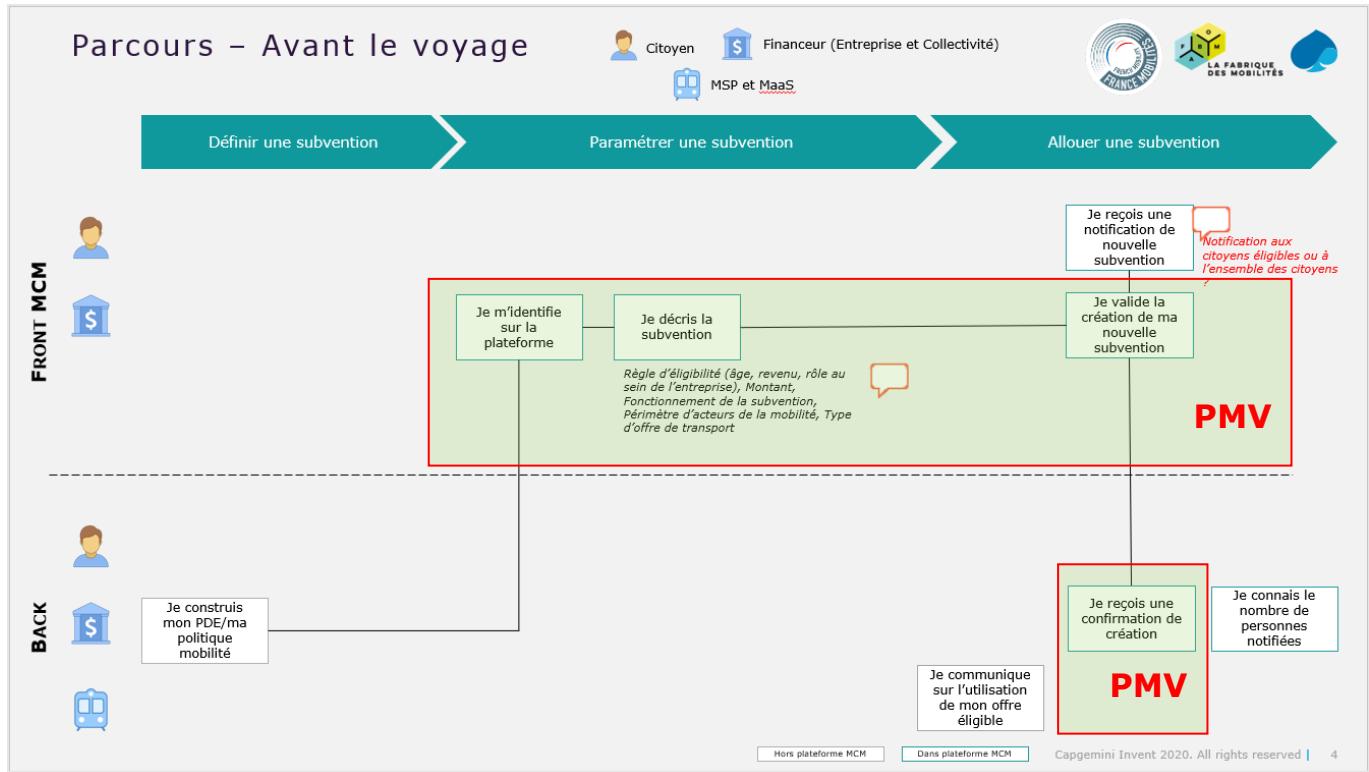
3.3.2. Processus « Initialisation du service »



Précisions :

- L'appartenance du citoyen à l'entreprise ou collectivité peut être certifiée par réception sur l'adresse email professionnelle d'un lien d'affiliation. C'est un moyen de certification moins fort que celui de s'intégrer directement au SI du financeur mais au regard du ratio difficulté d'intégration/niveau de certification, cette solution a été retenue comme satisfaisante pour ce PMV.
- La création de l'offre de mobilité sur la plateforme moB est uniquement à la main de l'administrateur moB. Le MSP/MaaS ou l'entreprise/collectivité ne peuvent pas créer leur offre directement sur moB.

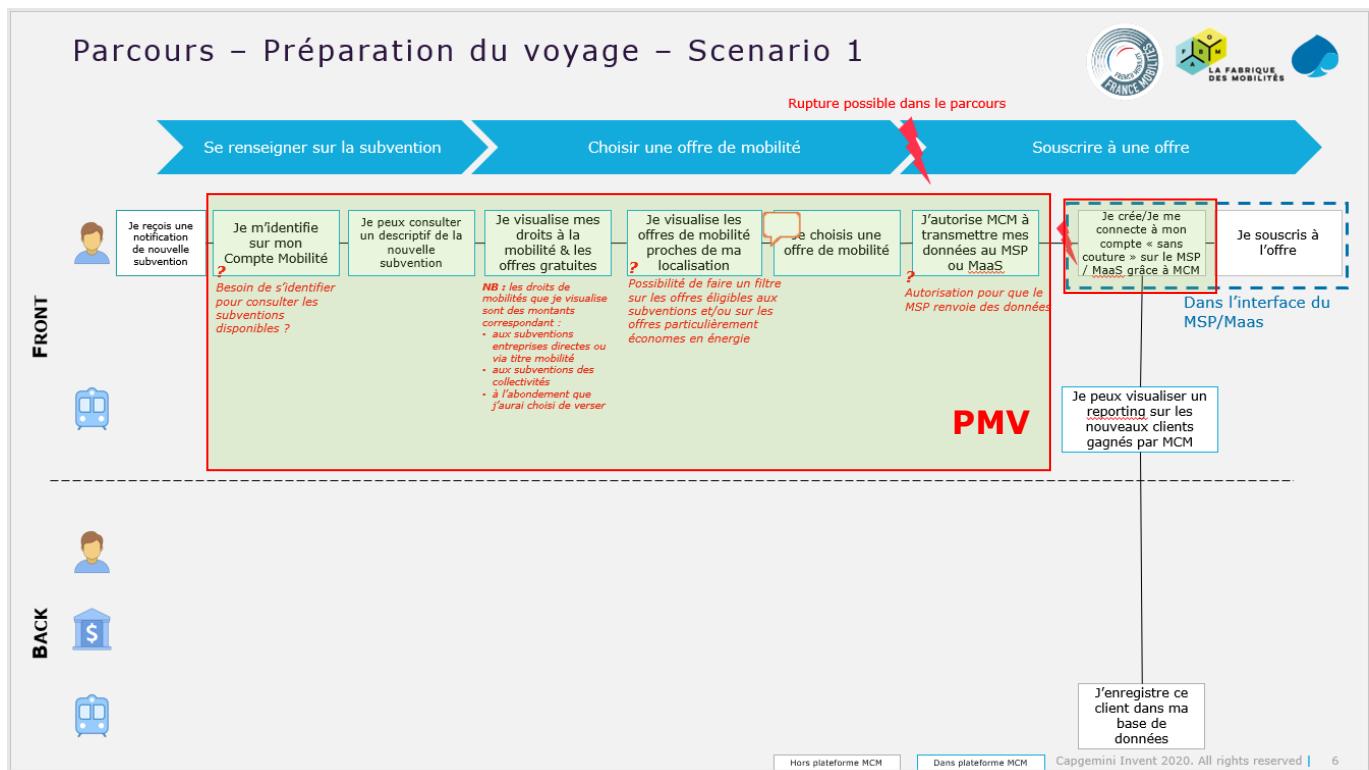
3.3.3. Processus « Avant le voyage »



Précisions :

- Les citoyens ne sont pas notifiés de la présence d'une nouvelle subvention.

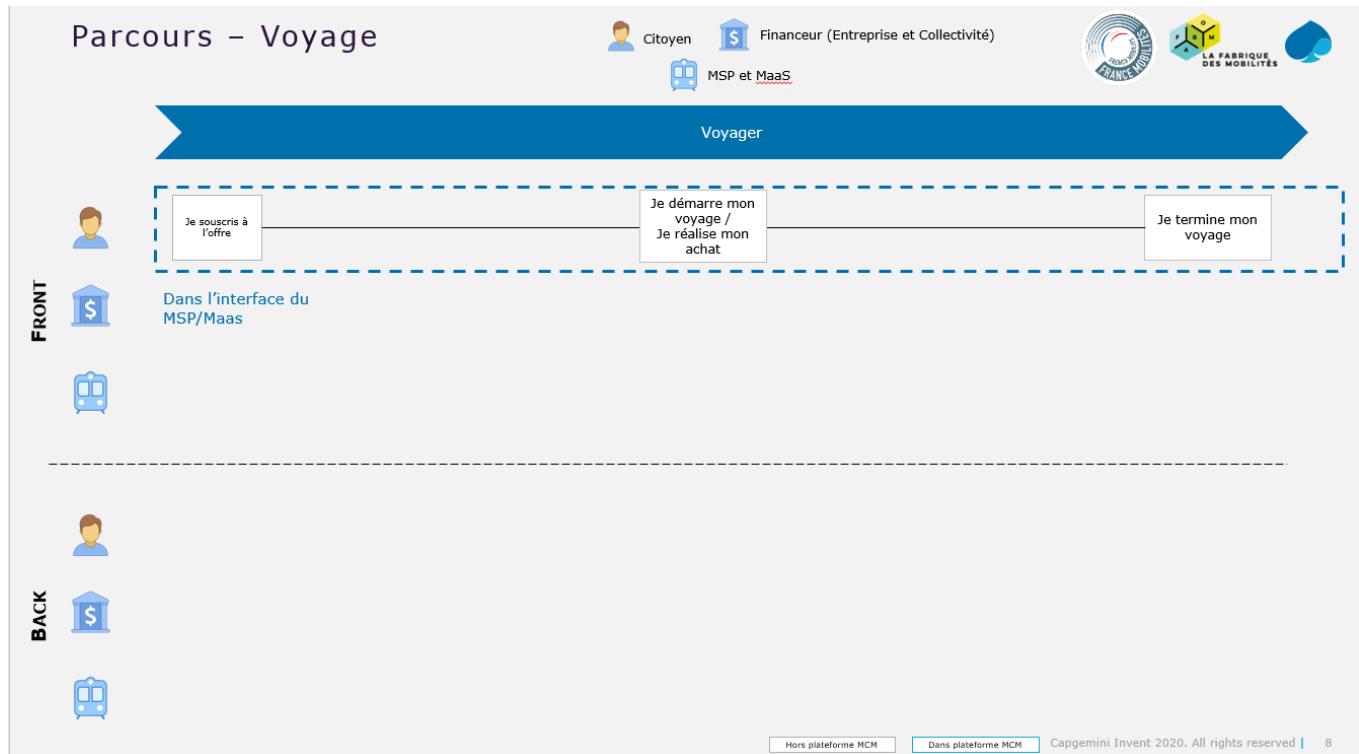
3.3.4. Processus « Préparation du voyage »



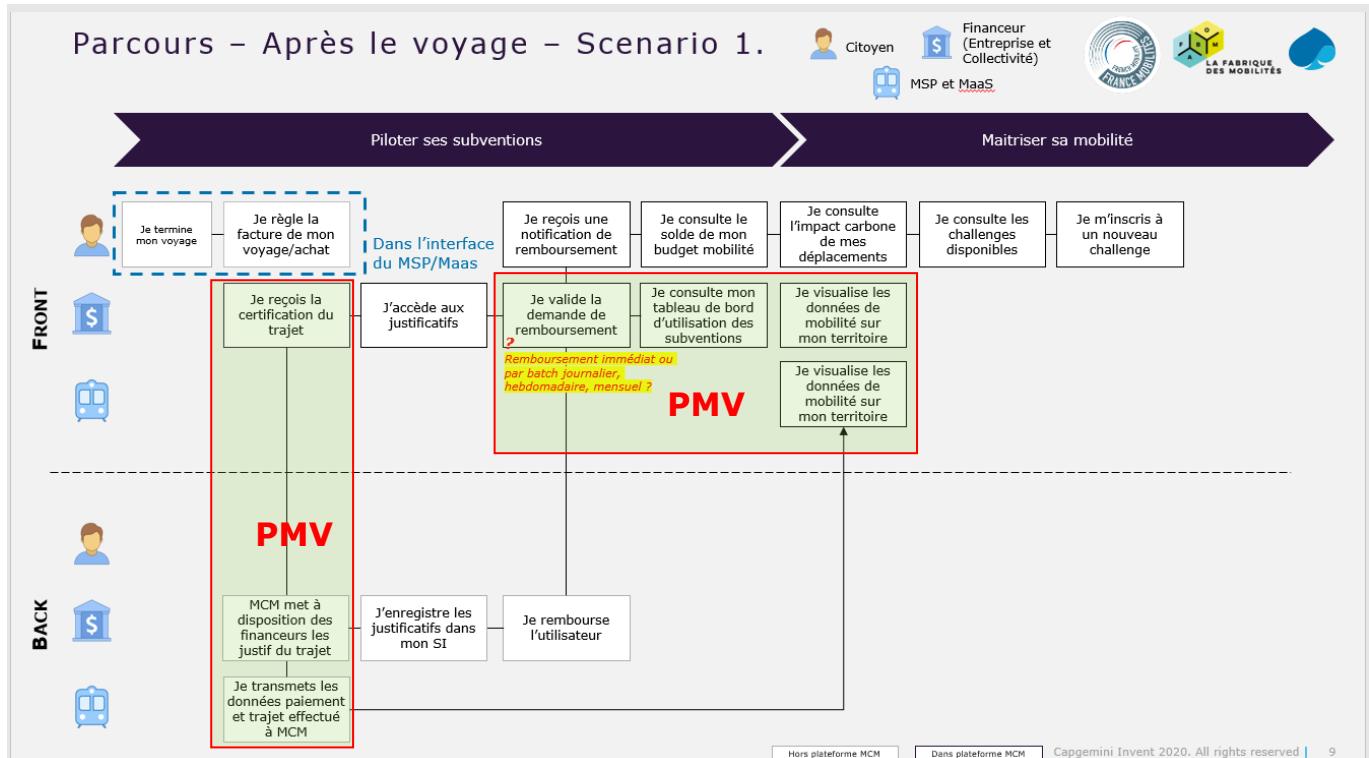
Précisions :

- La possibilité pour les citoyens de créer/se connecter sur le MPS/MaaS à partir du compte moB, que l'on peut nommer « moB Connect », nécessite l'ajout de moB en tant que fournisseurs d'identités externe à leur application. Cela permet la capitalisation sur les données du compte moB afin de créer/mettre à jour le compte MSP/MaaS nécessaire pour utiliser leurs services.

3.3.5. Processus « Voyage »



3.3.6. Processus « Après le voyage »



Précisions :

- Le MaaS / MSP peut joindre les données de paiement/facturation à une demande de 2 façons :
 - o Si le parcours de souscription est dans moB, il peut joindre des métadonnées de facturation en amont
 - o Si le parcours de souscription est dans le MaaS, ce dernier peut ajouter des documents de paiement/facture à la demande moB
- Le citoyen reçoit une notification de validation de la demande par moB. La notification de versement doit provenir du financeur.

3.4. Cas d'utilisation

3.4.1. Périmètre du PMV

Les cas d'usage suivant seront couverts par le PMV :

1. Inscription des MaaS, MSP, Collectivités, Employeurs, Citoyens / Salariés
2. Définition du catalogue d'offres de mobilité, information des usagers
3. Définition des communautés, définition des dispositifs incitatifs, affectation aux communautés
4. Affiliation des salariés à leur entreprise et validation des affiliations (manuelle ou automatique)
5. Demandes de subventions, soumission de justificatifs, approbation par l'organisme instructeur financeur
6. Obtention de données d'usage / rapports
7. Authentification auprès des MaaS/MSP via moB
8. Vérification d'identité / certification, obtention de preuves auprès de systèmes tiers (FranceConnect, DGFIP)

Sont en dehors du périmètre :

- La réservation, l'achat, la souscription de produits ou packages.
- L'encaissement, le paiement des fournisseurs, la facturation. L'ensemble des transactions ont lieu en dehors de Mon Compte Mobilité, dans les MaaS et MSP.

3.4.2. Vue d'ensemble des cas d'utilisation

Le diagramme de cas d'utilisation qui suit constitue une tentative de capturer l'ensemble du périmètre fonctionnel sous une forme synthétique et standard (UML). Il se lit de la façon suivante :

- La frontière du système que nous décrivons dans le présent dossier est représentée par un cadre.
- Un acteur est représenté par un bonhomme allumette.
- Deux acteurs peuvent être liés entre eux par une relation de généralisation/specialisation aussi nommée relation d'héritage représentée par une flèche dont l'extrémité est creuse. Elle se lit « *est un* » dans le sens de la flèche. Par exemple : « l'acteur Financeur *est un* Utilisateur Authentifié ».
- Chaque cas d'utilisation est représenté par une ellipse. Un usecase constitue la raison pour laquelle l'utilisateur souhaite interagir avec le système. Par exemple, « Gérer le contenu éditorial ».
- Un acteur peut être relié à un cas d'utilisation primaire par une ligne pleine non orientée. Dans ce cas, le usecase est primaire et la relation représente l'intention/la finalité de l'utilisateur. Par exemple, « en tant qu'Administrateur Fonctionnel MCM, je souhaite Gérer le contenu rédactionnel ».
- Un usecase primaire peut être lié à un ou plusieurs usecases secondaires à l'aide de flèches orientées, en pointillés. Cette relation est assortie d'un stéréotype « *include* » ou « *extend* » signifiant, respectivement, que le cas cible est obligatoire inclus/requis ou optionnellement étendu par le cas d'utilisation source. Par exemple, « Gérer le profil requiert une authentification préalable ». Autre exemple : « Afin moment de rejoindre une communauté, je peux soumettre un justificatif ».

Par ailleurs, nous avons opté pour le code couleur suivant :

- Apparaissent en vert tous les cas d'utilisation accessibles sans authentification préalable. Les fonctionnalités correspondantes sont par conséquent accessibles aux visiteurs anonymes, c'est-à-dire n'étant pas inscrit à Mon Compte Mobilité ou n'ayant pas saisi leurs identifiants/mots de passe.
- Nous avons représenté en rouge les cas d'utilisation disponibles uniquement après une authentification réussie.
- Enfin, les cas d'utilisation déclenchés en façon asynchrone ou par un acteur non humain (système externe ou ordonnanceur par exemple) ont été dépeints en violet.

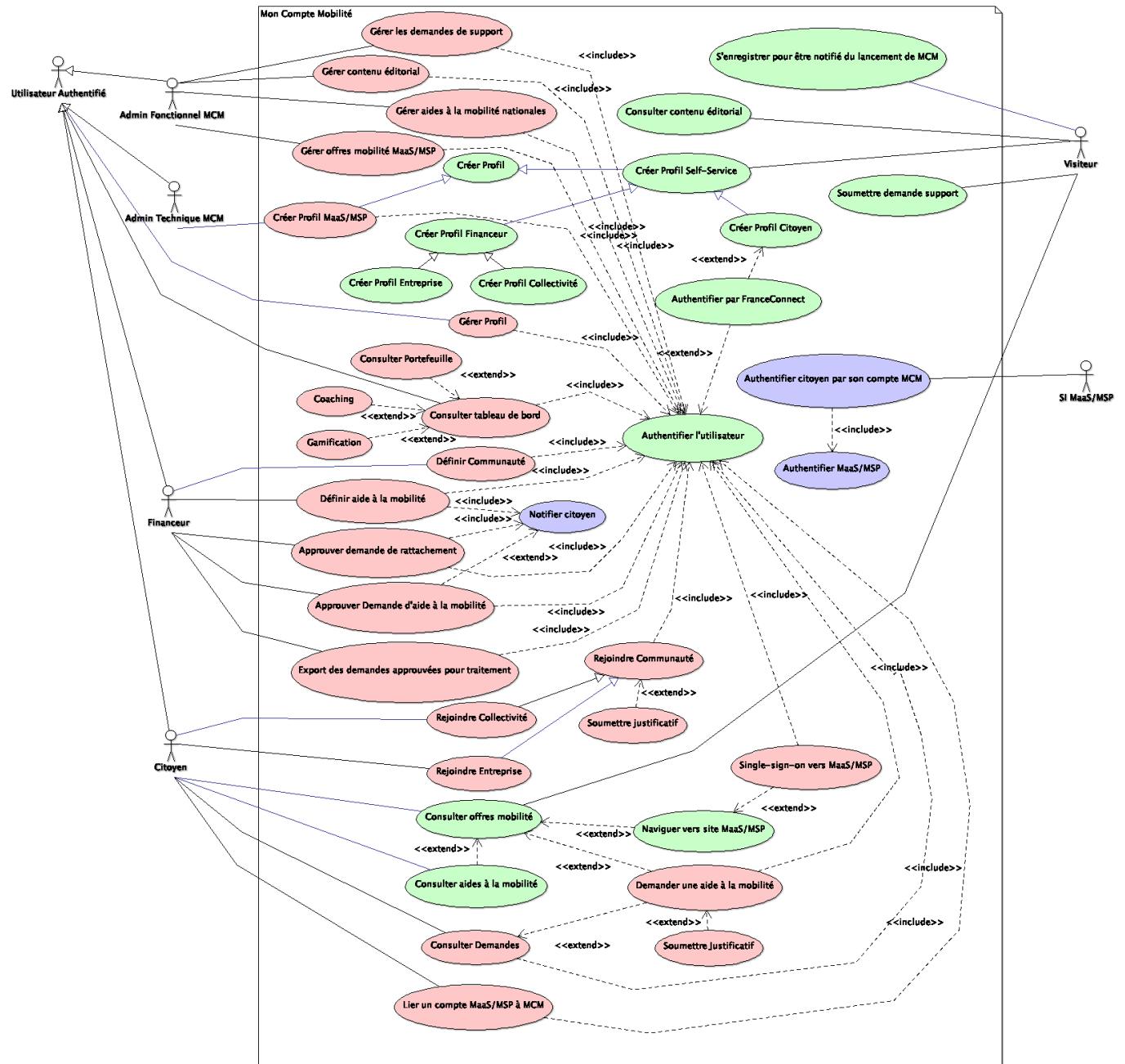


Figure 5 - Cas d'utilisation

3.4.3. Point de vue du visiteur

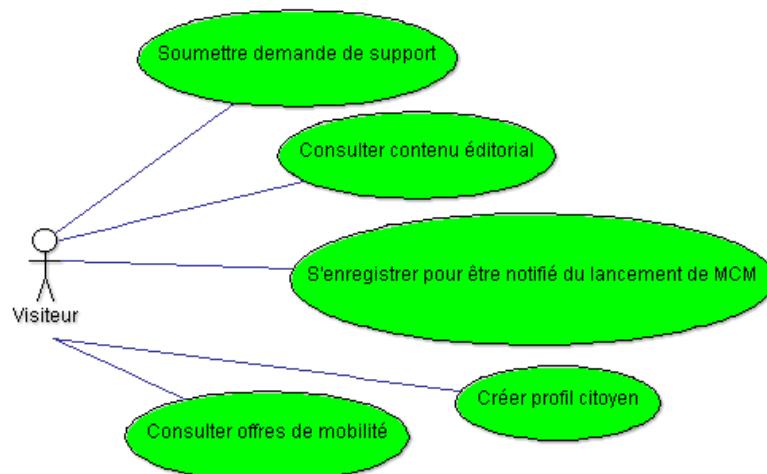


Figure 6 - Point de vue du visiteur

3.4.4. Point de vue du citoyen

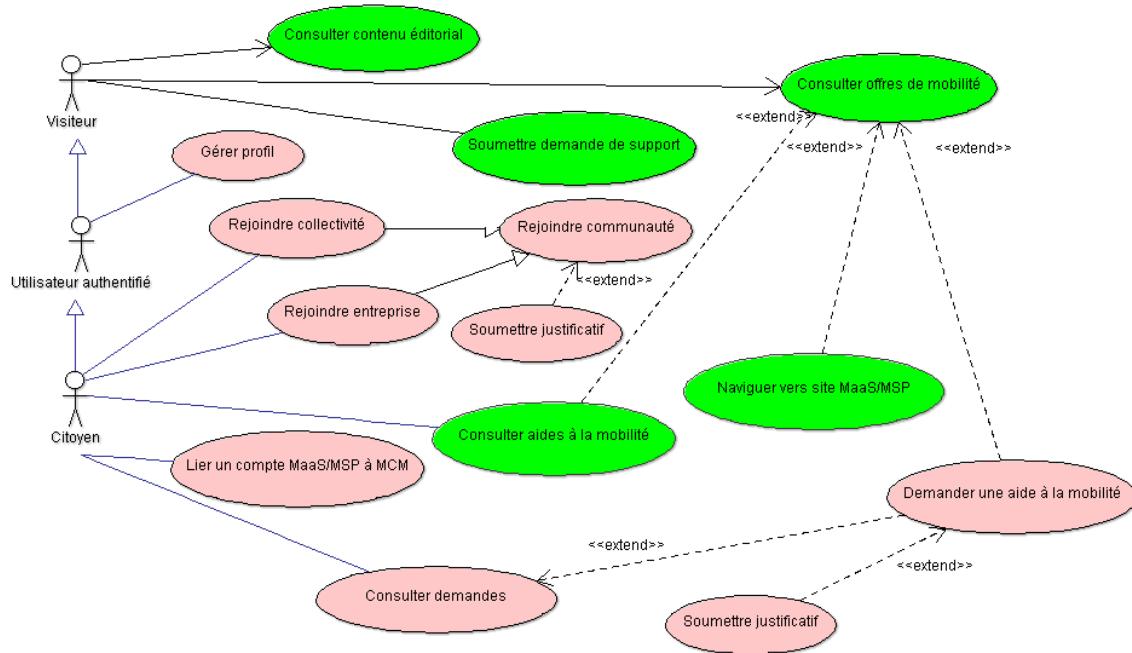


Figure 7 - Point de vue du citoyen

3.4.5. Point de vue du financeur

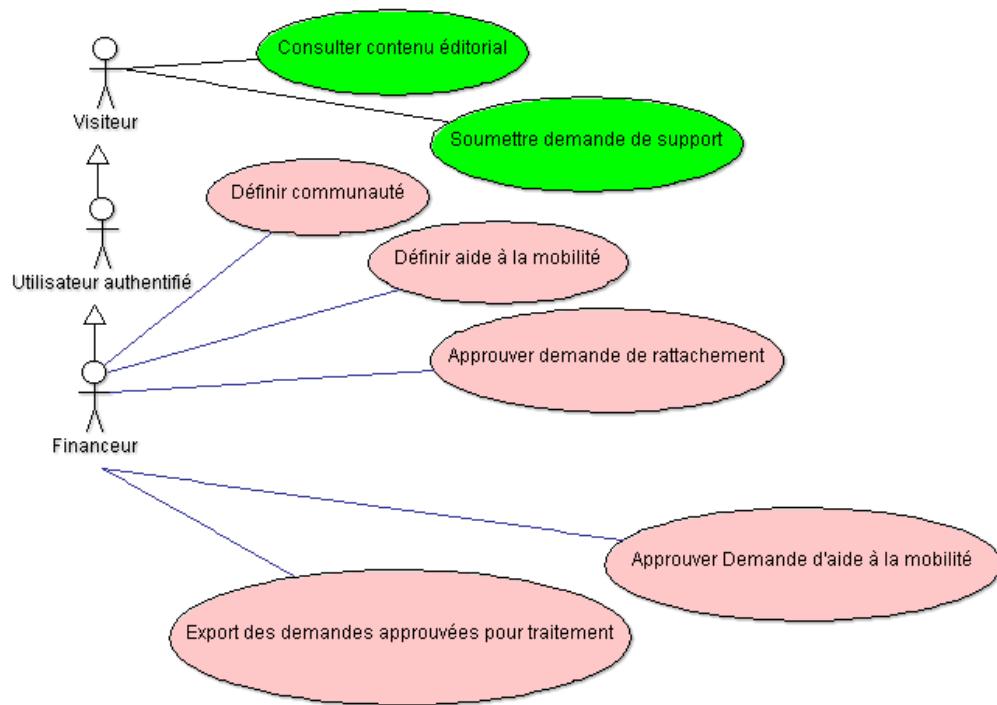


Figure 8 - Point de vue du financeur

3.4.6. Point de vue de l'administrateur fonctionnel

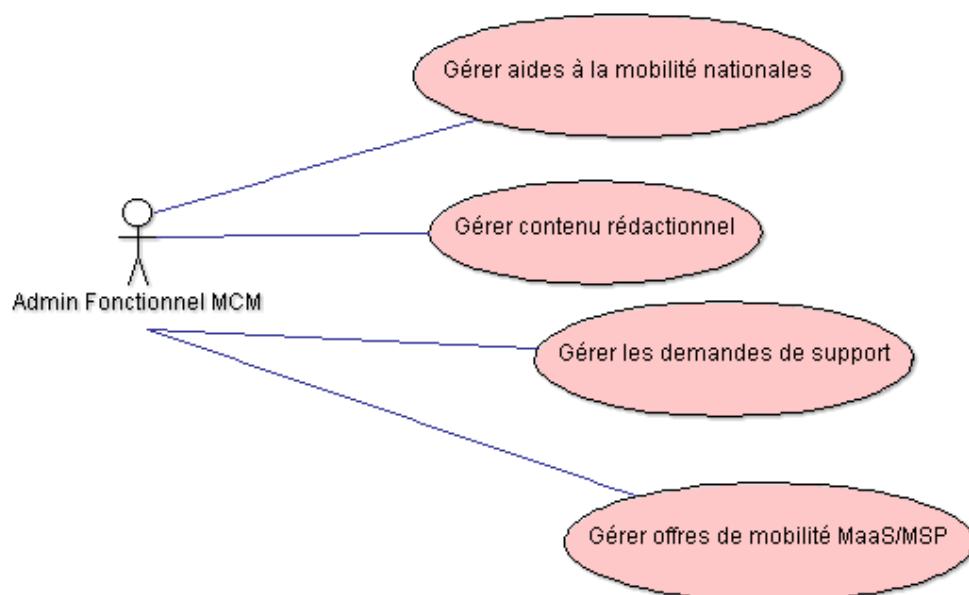


Figure 9 - Point de vue de l'administrateur fonctionnel

3.4.7. Point de vue de l'administrateur technique

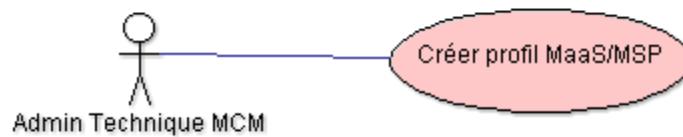


Figure 10 - Point de vue de l'administrateur technique

3.4.8. Traçabilité processus — cas d'utilisation

Le tableau ci-dessous établit la traçabilité entre les processus et les cas d'utilisation

Processus			Cas d'utilisation	
Acteur Métier	Processus Métier	Activité	Rôle	Cas d'utilisation
Citoyen	Initialisation du service	J'accède à Mon Compte Mobilité	Visiteur	Authentifier l'utilisateur Authentifier l'utilisateur par FranceConnect
		Je crée mon compte Je valide par mail la création de mon compte		Créer profil citoyen
		Je choisis les données que je veux partager en fonction des motifs et des acteurs	Citoyen	Gérer profil

		Je donne les informations validant l'appartenance à mon entreprise		Rejoindre entreprise Soumettre justificatif
		Je donne les informations validant l'appartenance à ma collectivité		Rejoindre collectivité Soumettre justificatif
Financeur	Initialisation du service	J'accède à Mon Compte Mobilité	Financeur	Authentifier l'utilisateur Authentifier l'utilisateur par FranceConnect
		Je crée mon compte Je valide par mail la création de mon compte	Financeur (Entreprise)	Créer profil entreprise
		Je crée mon compte Je valide par mail la création de mon compte	Financeur (Collectivité)	Créer profil collectivité
		Je transmets les données permettant d'identifier les membres de ma communauté	Financeur	Définir Communauté
MaaS MSP	Initialisation du service	J'accède à Mon Compte Mobilité	Administrateur technique moB Administrateur fonctionnel moB	Authentifier l'utilisateur Authentifier l'utilisateur par FranceConnect
		Je crée mon compte	Administrateur technique moB	Créer profil MaaS/MSP
		Je crée mon offre sur la plateforme	Administrateur fonctionnel moB	Gérer les offres de mobilités MaaS/MSP

Financeur	Avant le voyage	Je m'identifie sur la plateforme	Administrateur fonctionnel moB	Authentifier l'utilisateur Authentifier l'utilisateur par FranceConnect
		Je décris la subvention		Gérer aides à la mobilité nationales Définir offre de financement
		Je valide la création de ma nouvelle subvention		
		Je reçois une confirmation de création		
Citoyen	Préparation du voyage	Je m'identifie sur mon Compte Mobilité	Citoyen	Authentifier l'utilisateur Authentifier l'utilisateur par FranceConnect
		Je peux consulter un descriptif de la nouvelle subvention		Consulter aides à la mobilité
		Je visualise mes droits à la mobilité & les offres gratuites	Visiteur Citoyen	Consulter offres de mobilité
		Je visualise les offres de mobilité proches de ma localisation		
		Je choisis une offre de mobilité	Citoyen	Naviguer vers site MaaS/MSP Demander une aide à la mobilité Soumettre justificatif
		J'autorise MCM à transmettre mes données au MSP ou MaaS		Lier un compte MaaS/MSP à MCM
Citoyen	Après le voyage	Je consulte le solde de mon budget mobilité	Citoyen	Consulter demandes

Financeur		Je valide la demande de remboursement (souscription à l'offre de mobilité)	Financeur	Approuver demande de rattachement Approuver Demande d'aide à la mobilité
		Je consulte mon tableau de bord d'utilisation des subventions	Citoyen	Consulter Demandes
		Je visualise les données de mobilité sur mon territoire	Financeur	Export des demandes approuvées pour traitement

3.5. Cartographie fonctionnelle

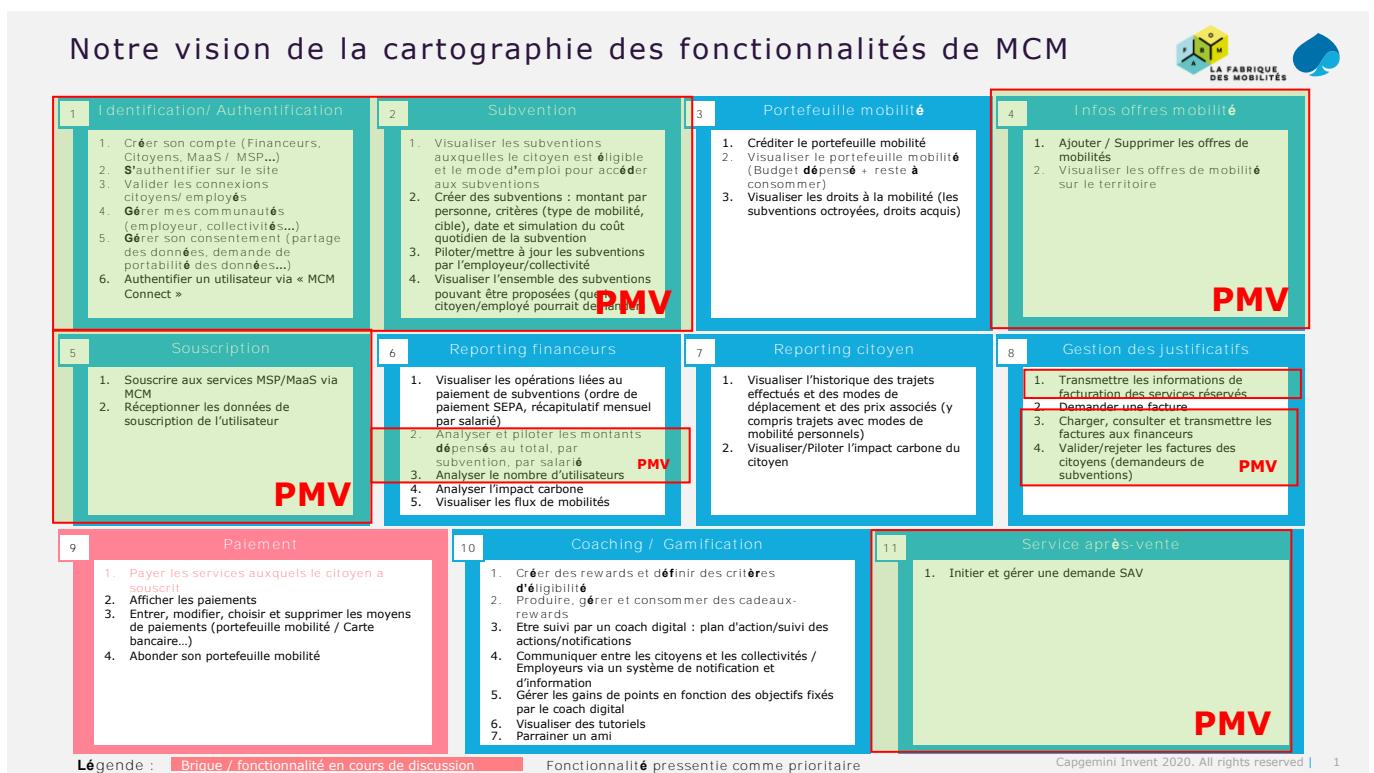


Figure 11 – Cartographie fonctionnelle

3.6. Principaux concepts métier

3.6.1. Diagramme et grille de lecture

Le diagramme ci-dessous constitue une tentative de synthétiser les entités manipulées par le système sous une forme normalisée (UML).

Il se lit de la façon suivante :

- Chaque concept clé ou entité est représenté par une boîte possédant 2 compartiments.
- Les entités peuvent être reliées par des **associations**. Nous avons recours dans le schéma à 3 types d'associations : la généralisation, la composition, l'agrégation.
- La **généralisation ou héritage** est représentée par une flèche pleine dont l'extrémité triangulaire est creuse. Elle se lit « est un » dans le sens de la flèche ou « se spécialise en » dans le sens inverse. Par exemple « Un financeur est un utilisateur ».
- La **composition** est représentée par une ligne pleine terminée par un losange noir ci. Ce dernier caractérise l'entité la plus forte de la relation, celle qui possède l'autre. L'autre extrémité est l'entité faible dont le cycle de vie est totalement géré. Elle ne peut exister indépendamment. La relation se lit « est composé d'un » en partant de l'entité la plus forte. Par exemple « un financeur est composé de communautés ». Les communautés n'existent pas en dehors des financeurs qui les ont créées.
- L'**agrégation** est représentée par une ligne pleine terminée par un losange vide. Ce dernier caractérise l'entité la plus forte de la relation, celle qui référence l'autre. L'entité faible existe en tant que telle indépendamment de l'entité forte. Cette dernière ne possède que des références aux entités qu'elle agrège. La relation se lit « a un ». Par exemple, « une demande d'octroi de dispositif incitatif a zéro ou N justificatifs ». La demande d'octroi ne gère pas le cycle de vie du justificatif. En d'autres termes, la suppression de la demande n'entraîne pas nécessairement la disparition du justificatif. Ce dernier peut exister en l'absence de demande. En particulier, le justificatif peut être partagé avec d'autres demandes ou d'autres types d'entités, l'Incitation Octroyée par exemple.
- Enfin, une instance d'association peut porter une information qui n'existe dans aucune de ses extrémités. C'est la notion de **classe d'association**. Par exemple, la relation Dispositif Incitatif — Communauté est assortie d'une Condition. La Condition ne fait pas partie du Dispositif, ni de la Communauté. C'est la relation entre une communauté particulière et un dispositif spécifique associé qui porte la condition.

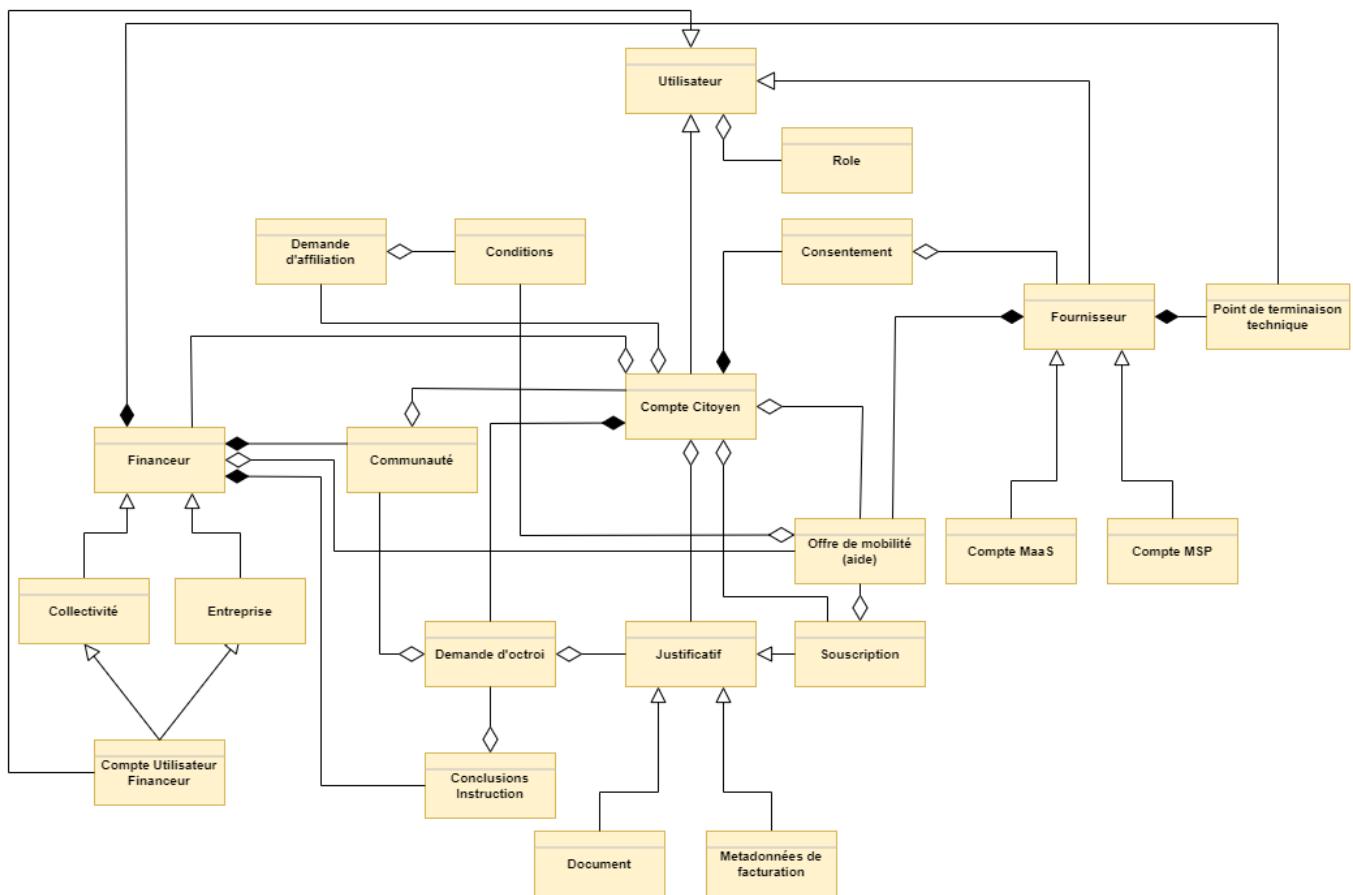


Figure 12 – Principaux concepts métiers

3.6.2. Description des entités

Les concepts clés sont décrits de façon plus détaillée dans les paragraphes qui suivent.

Utilisateurs

- **L'utilisateur** est un objet central du système. Il est instancié et persisté lorsqu'un visiteur initialement anonyme choisit de créer un compte dans moB. Il est possible de créer un compte à l'aide d'un email et d'un mot de passe stockés par moB. Dans ce cas moB est référentiel. Une autre méthode d'inscription consiste à s'authentifier via [FranceConnect](#). Dans ce cas, moB conserve une référence vers le fournisseur d'identité externe qui a permis d'initialiser le compte.
 - Il existe 3 types de comptes qui sont autant de spécialisations de l'entité Utilisateur : les Fournisseurs de mobilité (MaaS/MSP), les Financeurs et les Citoyens.

Fournisseurs et offres de mobilité

- Les comptes de type **Fournisseurs de mobilité** se subdivisent à leur tour en 2 catégories : les **comptes de MSP** et les **comptes de MaaS**. Les MaaS se comportent comme des agrégateurs de MSP.

- Les fournisseurs de mobilité proposent des **Offres de mobilité**.

Points de Terminaison Techniques

- Les Fournisseurs de mobilité possèdent généralement une vitrine accessible via Internet au travers d'une application mobile et vers laquelle moB devra rediriger les utilisateurs.
- Les Fournisseurs de mobilité sont également susceptibles d'exposer des **Points de Terminaison Techniques**, idéalement des APIs grâce auxquelles moB pourra obtenir des informations ou exécuter des transactions.
- Les Fournisseurs de mobilité intègrent le compte moB comme prérequis d'accès aux dispositifs d'incitation accessibles via moB, voire ajoutent moB comme moyen d'authentification sur leur système (moB Connect).
- Les Fournisseurs de mobilité intègrent les écrans moB dans leurs parcours client et/ou les APIs moB.

Financeurs, Collectivités et Entreprises

- Les **Financeurs** représentent une seconde catégorie d'utilisateurs.
- Nous distinguons deux sous-catégories constituées des **Collectivités** et des **Entreprises**. Les **Comptes de Collectivités** et les **Comptes d'Entreprises** sont identifiés par un numéro SIREN.

Communautés, Conditions et Consentement

- Les Financeurs peuvent définir des **Communautés**.
- Leurs membres sont éligibles à des offres de mobilité spécifiées sous certaines **Conditions**.
- Il existe également un **autre type de condition** qui concerne les champs spécifiques qui pourraient être rajoutés à une offre de mobilité (aide) et qui seraient spécifiques qu'à cette aide (Ex. rajouter dans le formulaire de demande d'aide le nombre de kilomètres parcouru)
- Les **conditions spécifient des critères d'éligibilité** et la nature des justificatifs qui devront être produits afin de bénéficier d'une aide.
- Le citoyen donne son **consentement** lors de la création de son compte.
- Un consentement est également lié à une demande d'aide : consentement au moment de la souscription à une aide pour le partage des données.
- Le consentement d'un citoyen est défini lors de la création de son compte (dans le formulaire via des checkbox) et lors de l'association de son compte à un compte de fournisseur de mobilité (acceptation des données/fonctionnalités partagées).

Citoyens

- Les **Citoyens** constituent la 3^{ème} et dernière classe d'utilisateurs.
- Un citoyen renseigne la **communauté** à laquelle il appartient (si configurée sur le financeur de l'aide) lorsqu'il fait sa demande de **souscription**.
- Via son compte, un citoyen peut souscrire à une **offre de mobilité** (aide) et peut uploader des **pièces justificatives** pour les joindre à sa demande
- Lorsqu'un citoyen est affilié à une entreprise, le catalogue d'aides qui lui est affiché se voit enrichi des offres de celles-ci.

Demandes d’Affiliation

- Afin d’être rattaché à un organisme financeur, le citoyen soumet une **Demande d’Affiliation**.
- Elle prend la forme d’une classe d’association reliant le citoyen au financeur. Elle possède un état reflétant le statut/l’avancement de l’instruction par le financeur.
- Une fois l’affiliation confirmée, les communautés (si paramétrées) auxquelles fait partie le citoyen sont connues.

Demande d’Octroi d’une incitation et Justificatifs

- Pour bénéficier d’un dispositif donné, le citoyen peut sous certaines conditions soumettre une **Demande d’Octroi**.
- L’éligibilité au dispositif est déterminée par l’appartenance à au moins une communauté concernée par le dispositif.
- Les critères que doit respecter le citoyen et les **Justificatifs** qui doivent être rattachés à la demande sont conditionnés par les communautés auxquelles appartient le demandeur.
Les justificatifs peuvent prendre plusieurs formes : des **Documents** fournis par le citoyen, la **Souscription** à une offre de mobilité confirmée par un MaaS/MSP, un ou plusieurs **Déplacements** certifiés.
- Les justificatifs ne sont visibles que par le financeur. Le citoyen ne fait qu’uploader ses justificatifs mais ne pourra pas les visualiser. Seuls les noms des justificatifs rattachés à ses sont visibles lorsqu’il récupère ses données au format fichier Référentiel et identification des entités.

3.6.3. Référentiel et identification des entités

Cette partie se focalise sur l’identification et le cycle de vie des entités.

Le référentiel des entités peut être interne ou externe au système moB.

Certaines entités n’existent que dans moB, leur cycle de vie est par conséquent totalement pris en charge par moB.

D’autres se situent à la frontière entre moB et des systèmes d’information externes.

C’est le cas par exemple des utilisateurs, des communautés, voire des offres de mobilité.

Si les fournisseurs de mobilité ou les financeurs n’ont pas de SI accosté à moB, alors la gestion de ces entités se fera dans moB qui sera alors référentiel.

Si un SI externe existe, les utilisateurs et communautés ne sont connus de moB que par identifiants externes.

Entité	Stockage dans le référentiel MCM	Source
Citoyen	Profil/Compte Citoyen	Salarié d’une entreprise Usager d’une collectivité
Financeur	Profil/Compte financeur	Système d’identification du répertoire des entreprises de l’INSEE (Institut national de la statistique et des études économiques)
Offre de mobilité	Contenu rédactionnel de l’offre de mobilité	Offre de mobilité définie par une entreprise

		Offre de mobilité définie par une collectivité
Aide à la mobilité	Contenu rédactionnel de l'aide à la mobilité	Aide à la mobilité définie par une entreprise Aide à la mobilité définie par une collectivité Aide à la mobilité définie par l'Etat (ou par une extra-territorialité)
Justificatif de rattachement	Justificatif (document électronique)	Préfecture, pôle emploi, fournisseur d'énergie, bulletin de salaire, assurance maladie (attestation d'invalidité), attestation sur l'honneur, centre des finances (revenu fiscal de référence)
Paiement	N/A	Banque
Support utilisateur	Support utilisateur	moB

Aucun objet transient, qui serait créé par moB mais n'y serait pas stocké, n'a été identifié.

Au même titre que les autres entités du système, il est nécessaire que chaque utilisateur soit identifié de façon unique.

Ces identifiants pourront être :

- Visibles de façon externe aux usagers, par exemple pour se connecter au système à travers un processus d'authentification ;
- Visibles de façon externe aux financeurs pour associer des usagers à leurs communautés ;
- Internes, manipulés uniquement par le système pour associer les données de transaction/d'usage remontées par les MSP aux comptes des usagers par exemple.

Nous étudierons dans les paragraphes ci-après les cas particuliers des entités représentant des utilisateurs.

Citoyens et employés

Les usagers devraient pouvoir créer leur compte quand bon leur semble et choisir un identifiant externe pertinent pour eux. Il pourrait s'agir d'une ou plusieurs adresses email personnelles ou professionnelles.

Il est à noter que :

- Tous les usagers ne seront pas nécessairement salariés
- Qu'ils peuvent avoir plusieurs employeurs simultanément et successivement
 - o Le cas de plusieurs employeurs simultanément n'est pas supporté
- Qu'un employeur n'attribue pas nécessairement d'adresse email à ses salariés.

Il n'est pas possible de s'appuyer sur le « Numéro de sécurité sociale », formellement Numéro d'Inscription au Registre des Personnes Physiques (NIR/NIRPP) car ce cadre d'utilisation n'est pas prévu selon le décret n°2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

Voir <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038396526?r=3cAsRPKW07>.

En effet, les domaines couverts sont uniquement :

- La protection sociale, la santé ;
- Le travail et l'emploi du secteur privé et du secteur public ;
- Le domaine financier, fiscal et douanier ;
- La justice ;
- Les statistiques publiques et le recensement ;
- L'éducation ;
- Le logement ;
- La prise en charge des victimes des essais nucléaires.

Entreprises et établissements

Les entreprises et les établissements possèdent un identifiant unique attribué par l'INSEE au sein du système d'identification du répertoire des entreprises de l'INSEE (Institut national de la statistique et des études économiques).

Le numéro SIREN est un code INSEE qui sert à identifier une entreprise, un organisme ou une association ayant des activités en France.

Le numéro SIRET est un code INSEE permettant l'identification d'un établissement ou d'une entreprise française.

Une entreprise peut avoir plusieurs établissements.

Un dispositif peut être associé soit à un groupe (donc à tous ses établissements) soit à un établissement.

Collectivités

Les collectivités ont une obligation d'avoir un SIREN/SRET depuis la circulaire CIRCULAIRE n° NOR/MCT/B/07/00004/C du 8 janvier 2007.

Les collectivités ont une obligation d'avoir un SIREN/SRET. depuis la circulaire CIRCULAIRE n° NOR/MCT/B/07/00004/C du 8 janvier 2007.

Extrait de la circulaire CIRCULAIRE n° NOR/MCT/B/07/00004/C du 8 janvier 2007 :

(...)Le décret n° 83-121 du 17 février 1983 modifiant le décret n° 73-314 du 14 mars 1973 a étendu à toutes les personnes morales de droit privé et public et aux institutions et services de l'Etat ou des collectivités territoriales, le champ d'application du système national d'identification et d'un répertoire des entreprises et de leurs établissements.

(...)

Un numéro d'identification SIREN à 9 chiffres est attribué à toute collectivité territoriale, à tout établissement public ainsi qu'aux institutions et services de l'Etat.

Un identifiant SIRET à 14 chiffres : Siren + nic (n° interne de classement) est attribué aux établissements secondaires : implantations géographiques distinctes des services de l'organisme public où s'exerce tout ou partie de l'activité de l'organisme. Par dérogation plusieurs établissements peuvent être immatriculés à la même adresse, c'est le cas notamment des services qui reçoivent du public, une bibliothèque municipale et une salle de spectacle auront chacune un N° SIRET même si elles sont situées à la même adresse. Pour répondre à des besoins de gestion de la direction de la comptabilité publique, les budgets annexes de collectivité territoriale ou d'établissements hospitaliers possèdent aussi leurs sirets.

(...) Le décret n°83-121 du 17 février 1983 modifiant le décret n°73-314 du 14 mars 1973 a étendu à toutes les personnes morales de droit privé et public et aux institutions et services de l'Etat ou des collectivités territoriales, le champ d'application du système national d'identification et d'un répertoire des entreprises et de leurs établissements.

(...)

Un numéro d'identification SIREN à 9 chiffres est attribué à toute collectivité territoriale, à tout établissement public ainsi qu'aux institutions et services de l'Etat.

Un identifiant SIRET à 14 chiffres : Siren + nic (n° interne de classement) est attribué aux établissements secondaires : implantations géographiques distinctes des services de l'organisme public où s'exerce tout ou partie de l'activité de l'organisme. Par dérogation plusieurs établissements peuvent être immatriculés à la même adresse, c'est le cas notamment des services qui reçoivent du public, une bibliothèque municipale et une salle de spectacle auront chacune un N° SIRET même si elles sont situées à la même adresse. Pour répondre à des besoins de gestion de la direction de la comptabilité publique, les budgets annexes de collectivité territoriale ou d'établissements hospitaliers possèdent aussi leurs sirets.

MaaS, MSP

Les MaaS/MSP sont identifiés par un SIREN/SIRET s'il s'agit d'une entreprise, d'une association ou d'un organisme ayant une activité en France.

L'URL du service sera stockée pour permettre la redirection depuis la liste des offres de mobilité. Son identifiant technique est le nom du client.

Communautés

Ce sont les groupes de citoyens éligibles à une certaine offre de remboursement, subvention et/ou abondement.

Elles sont définies par les financeurs qui y attachent des droits.

Les citoyens les rejoignent lorsqu'ils créent leurs comptes.

Ce sont les groupes de citoyens éligibles à une certaine offre de remboursement, subvention et/ou abondement.

Elles sont définies par les financeurs qui y attachent des droits.

L'usurpation d'identité doit être empêchée. Il faut s'assurer que le salarié qui crée le compte travaille bien dans l'entreprise au moment où il crée le compte.

Cela implique un process de validation du côté de l'entreprise : manuel ou automatique.

A minima, un process manuel : l'entreprise possède un compte et quelqu'un est en charge de valider les ralliements à la communauté (et les demandes d'aides à la mobilité).

Idéalement, le process automatique : l'utilisateur est invité à répondre à un challenge.

Par exemple, s'authentifier auprès du SI de l'entreprise. Le fournisseur d'identité est alors en mesure de retourner des attributs de l'utilisateur qui pourront plus tard être exploitées pour valider les droits.

Ce cas est courant dans le cas d'une entreprise : par exemple avec office.com utilise l'authentification auprès des SI des entreprises.

3.7. Exigences fonctionnelles

3.7.1. Authentification unique

La valeur de moB réside dans le fait de simplifier l'accès aux dispositifs d'incitation à la mobilité douce, en fine aux offres des MaaS et MSP.

L'usager ne devrait pas se voir soumettre un nouveau cycle défi-réponse lorsqu'il navigue vers un nouveau service depuis moB.

De même, l'authentification par FranceConnect doit être présente afin d'apporter un haut niveau de certification d'identité du compte, empêcher les doublons et limiter la fraude.

3.7.2. Durée de rétention des données (hors RGPD)

Documents

Les livres et les registres comptables, ainsi que les pièces justificatives doivent être conservés pendant 10 ans (source : [Ministère de l'Economie](#)).

Cela concerne les justificatifs de facturation attachés aux souscriptions.

Données d'éligibilité CEE

Les preuves permettant de justifier l'éligibilité au programme CEE accordée à MCM, doivent être conservées (source : [Ministère de l'Ecologie](#)).

3.7.3. Conformité RGPD

Identification des données personnelles

Les données personnelles identifiées dans le cadre du PMV dans le document [[R05](#)] sont :

- Adresse de domicile personnel
- Adresse email personnelle
- Attestation d'inscription à Pôle emploi
- Attestation sur l'honneur
- Avis d'imposition
- Carte invalidité
- Code postal
- Composition du foyer fiscal
- Consentement au partage de données personnelles
- Date de naissance
- Géolocalisation
- Identité citoyen (nom, prénoms)
- Justificatif de domicile
- Justificatifs d'identité
- Mot de passe
- Niveau de revenus de l'employé

- Numéro de téléphone
- Permis de conduire
- Revenu fiscal de référence

Information des personnes concernées (traitement loyal et transparent)

Le RGPD impose une information complète et précise (source [CNIL](#)).

La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

Pour les responsables de traitement, elle contribue à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

MCM informera les utilisateurs en cas de collecte directe, et au moment de la collecte directe, ou en cas de collecte indirecte des données, dès que possible. L'information sera également faite en cas de modification substantielle ou d'événement particulier (exemples : changement dans les modalités d'exercice des droits, violation de données, etc.).

L'information délivrée doit être « concise, transparent, compréhensible et aisément accessible, en des termes clairs et simples » : utiliser un vocabulaire simple, faire court et lisible, garantir l'accessibilité de l'information, adapter l'information au public visé, aux situations et aux supports.

Dans tous les cas, les informations à fournir sont l'identité et les coordonnées de MCM, les finalités, la base légale, le caractère obligatoire ou facultatif du recueil des données, les destinataires ou catégories de destinataires des données, le droit des personnes concernées, les coordonnées du délégué à la protection des données et le droit d'introduire une réclamation auprès de la CNIL, ainsi qu'en cas de collecte indirecte, la catégorie et la source des données.

Exercice des droits d'accès et à la portabilité

Afin que les utilisateurs puissent faire valoir leur droit à la portabilité, moB devra leur permettre de récupérer leurs données (pour leur usage personnel ou pour les transmettre à un tiers de leur choix).

Les données concernées sont celles recueillies avec accord des utilisateurs et également des données tirées de l'activité de moB.

moB fournira ces données dans un format « structuré, couramment utilisé et lisible par la machine », comme par exemple dans un format CSV, JSON, vCard, etc.

Le droit d'accès donne aux utilisateurs la possibilité d'exercer leur curiosité sur les données détenues par moB, d'en demander la rectification ou l'effacement.

Les données non réutilisables restent susceptibles d'être remises aux utilisateurs dans un format « lisible par un humain » dans le cadre du droit d'accès, comme par exemple un pdf.

(source : <https://www.cnil.fr/fr/le-droit-la-portabilite-obtenir-et-reutiliser-une-copie-de-vos-donnees>)

Exercice des droits de rectification et d'effacement

Le droit de rectification permet aux utilisateurs de corriger des données inexactes ou de compléter des données en lien avec la finalité du traitement.

De même, les utilisateurs peuvent demander l'effacement si au moins une situation apparaît :

- leurs données sont utilisées à des fins de prospection ;
- leurs données ne sont pas ou plus nécessaires au regard des objectifs pour lesquelles elles ont été initialement collectées ou traitées ;
- les utilisateurs retirent leur consentement à l'utilisation de leurs données ;
- leurs données font l'objet d'un traitement illicite (par exemple, publication de données piratées) ;
- leurs données ont été collectées lorsque vous étiez mineur dans le cadre de la société de l'information (blog, forum, réseau social, site web...) ;
- leurs données doivent être effacées pour respecter une obligation légale ;
- les utilisateurs s'opposent au traitement de leurs données et le responsable du fichier n'a pas de motif légitime ou impérieux de ne pas donner suite à cette demande.

Pour ce faire, moB fournira un accès sur la page d'information réservée à l'exercice de ces droits sur le site web (« politique confidentialité », « politique vie privée », « mention légales », etc.) à travers un formulaire.

(source : <https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations>)

(source : <https://www.cnil.fr/fr/le-droit-leffacement-supprimer-vos-donnees-en-ligne>)

Exercice du droit de limitation du traitement

Les utilisateurs ont la possibilité de demander à MCM de geler l'utilisation de leurs données. Concrètement, MCM ne devra plus utiliser les données mais devra les conserver ou de les conserver en cas de volonté d'effacement de la part de MCM.

(source : <https://www.cnil.fr/fr/le-droit-la-limitation-du-traitement-geler-lutilisation-de-vos-donnees>)

Exercice du droit d'opposition

Les utilisateurs peuvent s'opposer à ce que leurs données soient utilisées par MCM pour un objectif précis. Les utilisateurs doivent mettre en avant « des raisons tenant à votre situation particulière », sauf en cas de prospection commerciale, à laquelle vous pouvez vous opposer sans motif.

Si la demande d'opposition ne concerne pas la prospection, MCM pourra justifier son refus au motif que :

- il existe des motifs légitimes et impérieux à traiter les données ou que celles-ci sont nécessaires à la constatation, exercice ou défense de droits en justice ;
- un contrat vous lie avec l'organisme ;
- une obligation légale lui impose de traiter vos données ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Pour ce faire, moB fournira un accès sur la page d'information réservée à l'exercice de ces droits sur le site web (« politique confidentialité », « politique vie privée », « mention légales », etc.) à travers un formulaire.

(source : <https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees>)

Sous-traitance : identifiée et contractualisée

Les données ne seront pas confiées à un prestataire.

Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne

Les données ne seront pas transférées en dehors de l'Union européenne. Elles sont stockées sur des infrastructures Azure en France.

Bases légales et traitements

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à moB de traiter des données à caractère personnel.

Il est permis de traiter des données personnelles lorsque le traitement repose sur une des 6 bases légales mentionnées à l'article 6 du RGPD :

- le consentement : la personne a consenti au traitement de ses données ;
- le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;
- l'obligation légale : le traitement est imposé par des textes légaux ;
- la mission d'intérêt public : le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- l'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées ;
- la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.

(source : <https://www.cnil.fr/fr/la-lieute-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd>)

Le choix d'une base légale pour un traitement donné mis en œuvre par moB a

Base légale	Conséquences
Contrat	Coopération du guichet unique. Le droit d'opposition ne peut pas s'exercer à l'égard des traitements fondés sur le contrat. Le droit à la portabilité des données peut quant à lui s'exercer à l'égard de ces traitements.
Mission d'intérêt général	Pas de soumission au guichet unique. Tous les droits des personnes concernées peuvent s'exercer à l'égard des traitements fondés sur la mission d'intérêt public, y compris le droit d'opposition, à l'exception du droit à la portabilité.
Intérêt légitime	Le droit à la portabilité ne peut pas s'exercer à l'égard des traitements fondés sur l'intérêt légitime. En revanche, une obligation de transparence renforcée est prévue pour ces traitements : la nature de l'intérêt légitime poursuivi par le responsable du traitement doit figurer dans les informations portées à la connaissance des personnes.
Consentement	Le consentement de l'utilisateur doit être libre, univoque (c'est-à-dire sans ambiguïté), spécifique à un traitement et à une finalité et éclairé (accompagné des informations de l'identité du responsable du traitement, des finalités

	<p>poursuivies, des catégories de données collectées, de l'existence d'un droit de retrait du consentement et le cas échéant, le transfert vers un pays hors Union européenne et l'utilisation des données dans le cadre de décisions individuelles automatisées).</p> <p>MCM devra fournir la possibilité de retrait du consentement ainsi que la preuve du consentement.</p> <p>En France, en-dessous de 15 ans, la loi « Informatique et Libertés » impose le recueil du consentement conjoint de l'enfant et du titulaire de l'autorité parentale.</p>
--	--

3.7.4. Fonctionnalités multiplateformes

Dans le cadre du PMV, les différents acteurs accèderont aux mêmes fonctionnalités de MCM soit par un navigateur web sur ordinateur ou sur navigateur mobile (responsive design).

MCM sera utilisable avec les dernières versions des navigateurs web [Chrome](#) et [Firefox](#).

3.8. Exigences non fonctionnelles

3.8.1. Volumétrie cible

Volumétries fournies par le GART.

ENTRANTS	PMV (Phase 1)	Cible basse (Phase 2)	Cible haute (Phase 2)
Nombre utilisateurs (citoyens / usagers)	20 000	100 000	1 000 000
dont chômeurs	1 620	8 100	81 000
dont situation de handicap	74	370	3 700
dont détenteurs du permis de conduire (B)	6 600	33 000	330 000

Phase 1 = expérimentation

Phase 2 = après 3 ans, échelle nationale

3.8.2. Rétention des données

Les durées de rétention des données sont précisées dans le document « MCM – Référentiel données et traitements » (cf. [[R05](#)]).

3.8.3. Portabilité

À l'issue de la phase d'expérimentation, le système moB devra être en capacité d'être transmis à un opérateur tiers. De même l'infrastructure post-phase d'expérimentation reste à définir.

- Nécessité de pouvoir transporter le système à moindre frais sur une infrastructure différente
- Nécessité de maîtriser (limiter ou identifier clairement) les adhérences au IaaS/PaaS

3.8.4. Performance

Aucune exigence de performance n'a été précisément établie.

Cependant, le site web doit répondre dans des temps acceptables pour l'utilisateur et ne bridant pas l'expérience. Les services APIs doivent être mesurés de répondre dans des temps de réponse suffisants aux systèmes utilisateur afin de ne pas impacter les fonctionnalités de ces derniers.

3.8.5. Disponibilité

La plage d'ouverture des services de MCM est de 24h24, 7j/7 hors interruptions programmées.

GTR/RTO : en cas de dysfonctionnement d'un composant d'infrastructure, le délai de remise en fonctionnement est de 12h

RPO : moB ne stocke pas de données critiques, l'expression d'un RPO faible est appropriée (4h de production)

Sauvegardes : la fréquence des sauvegardes est alignée sur le RPO

3.8.6. Confidentialité

- Chaque usager ne voit que ses propres données
- MaaS/MSP : accès aux scopes de données strictement nécessaires
- Aggrégation par identité pour les financeurs
- Aggrégation de données anonymisées pour les AOM

3.8.7. Données à caractère personnel

Stockage

moB effectue un regroupement des attributs personnels dans un stockage dédié.

Chiffrement

Les données sensibles doivent être chiffrées :

- Au repos / at Rest
- En transit / on motion

Le citoyen peut être amené à déposer des pièces justificatives sensibles (carte d'identité, passeport, ...) que le financeur est susceptible de demander.

- Afin de **garantir la confidentialité** des données transmises par l'usager, **seul le financeur doit** être en mesure de **consulter les pièces justificatives**
- Les **métadonnées** de souscription (de la demande) **ne font pas partie du périmètre de chiffrement** car elles ne sont pas jugées sensibles.

Suppression

Conformément au RGPD, tout utilisateur peut demander la suppression de ses données personnelles.

Portabilité

Même s'il n'existe pas de service équivalent à moB vers lequel les citoyens pourraient migrer leurs données, l'utilisateur doit pouvoir télécharger ses données sous une forme lisible.

3.8.8. Intégrité des données

Il existe 3 cas de figure à prendre en compte :

- S'assurer que les données ne sont pas altérées au repos
- Ni lors d'un transfert
- Au cours des transactions applicatives, les modifications doivent être atomiques

3.8.9. Traçabilité

Toute modification de l'état du système doit être journalisée.

Toute connexion doit être tracée.

Toute lecture d'information sensible.

Toute modification d'information sensible donne lieu à une notification.

Toute opération d'administration.

Format : Date / Emplacement / Identifiant acteur / Nom de l'opération / Nom de l'information consultée

3.8.10. Non répudiation

Rendue possible grâce aux traces/auditabilité.

3.8.11. Extensibilité

Le système moB doit être extensible et doit permettre :

- D'intégrer de nouveaux MaaS
- D'intégrer de nouveaux MSP
- De se mettre à jour sans indisponibilité, à chaud, par simple paramétrage

3.8.12. Déploiement progressif

Une nouvelle fonctionnalité doit pouvoir être expérimentée auprès d'une population déterminée (bassin géographique, entreprise, etc.).

3.8.13. Résilience

Le système étant par nature fortement connecté à des tiers, il doit résister à une défaillance de l'un des composants. Une panne ou une indisponibilité d'un tiers ne doit pas compromettre la stabilité de moB.

3.8.14. Démarche open source

La plateforme moB est un objet de bien commun, dont le code source sera en libre accès, sous une licence appropriée à la réutilisation et facilitant la contribution.

Les schémas d'architecture, ce DAT, le code source seront documentés et publiés selon des règles de validation et d'approbation préétablies.

4. Architecture logique

4.1. Architecture Hub

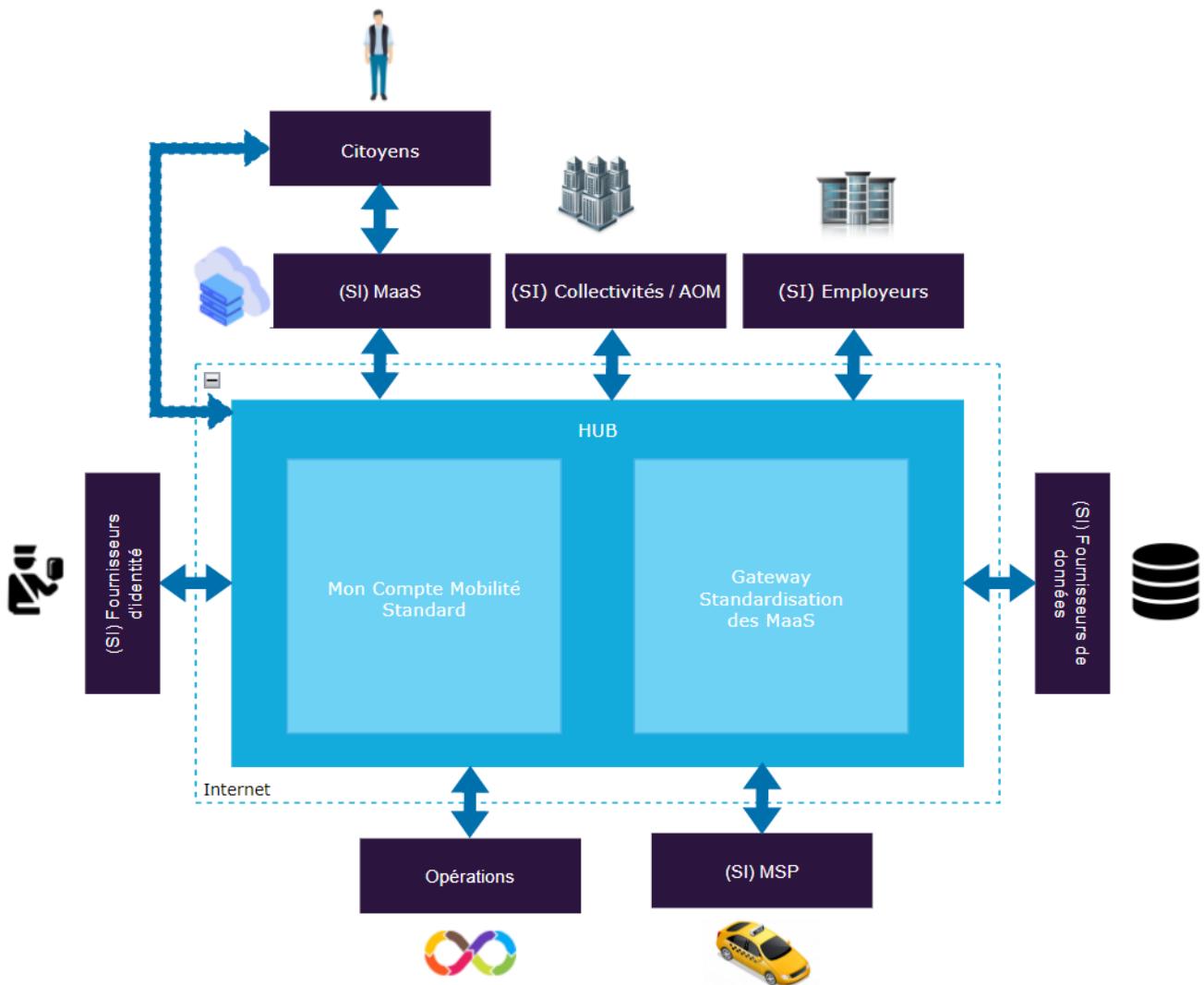


Figure 13 – Architecture générale

Le HUB Mon Compte Mobilité comporte à la fois Mon Compte Mobilité avec une extension standardisée de Mob dont ce DAT fait l'objet et la Gateway MCM Standardisation des MaaS.

Une caractéristique importante de ce HUB réside dans le fait qu'elle est susceptible d'initier de nombreuses interactions avec de multiples systèmes externes.

Nous avons présenté les principaux acteurs pouvant solliciter Mon Compte Mobilité : les Citoyens, les opérateurs humains intervenant au sein des Collectivités et des Employeurs affiliés. Les citoyens peuvent se connecter au HUB soit directement dans le cas de l'utilisation de leur compte Mob standard, soit par le biais d'un système externe (SI MaaS/MSP).

Outre les sessions interactives déclenchées via des interfaces homme-machine, Mon Compte Mobilité devra également servir et s'appuyer sur des SI externes : fournisseurs d'identité, fournisseurs de

données certifiées, SI des MaaS et des MSP. Par ailleurs, il est hautement désirable d'automatiser la validation des demandes d'affiliation et d'octroi de dispositifs incitatifs par des appels programmatiques aux SI des Collectivités et des Entreprises.

Enfin, des points d'accès sont provisionnés (bloc opérations), ils sont destinés aux équipes de développement et d'exploitation de la plateforme.

4.2. Sous-systèmes et dépendances

Un premier axe de décomposition du système réside dans le rôle que joueront ses composantes dans le déploiement.

Le problème présente une caractéristique géographique car — qu'il s'agisse des MaaS, des MSP, des financeurs ou des entreprises —, les différents acteurs et services sont rattachés à un territoire, possèdent une portée définie ou sont susceptibles d'être opérés localement. Par ailleurs, il est probable que certains territoires posséderont un existant dont il faudra tenir compte.

C'est pour toutes ces raisons que nous envisageons d'introduire un concept de HUB local afin de bénéficier d'un certain niveau d'isolation, des configurations et des extensions distinctes.

A l'inverse, un citoyen n'est supposé posséder qu'un seul compte de portée nationale. Ceci nous conduit à considérer un concentrateur global représenté ci-dessous par le sous-système libellé « Portail moB ».

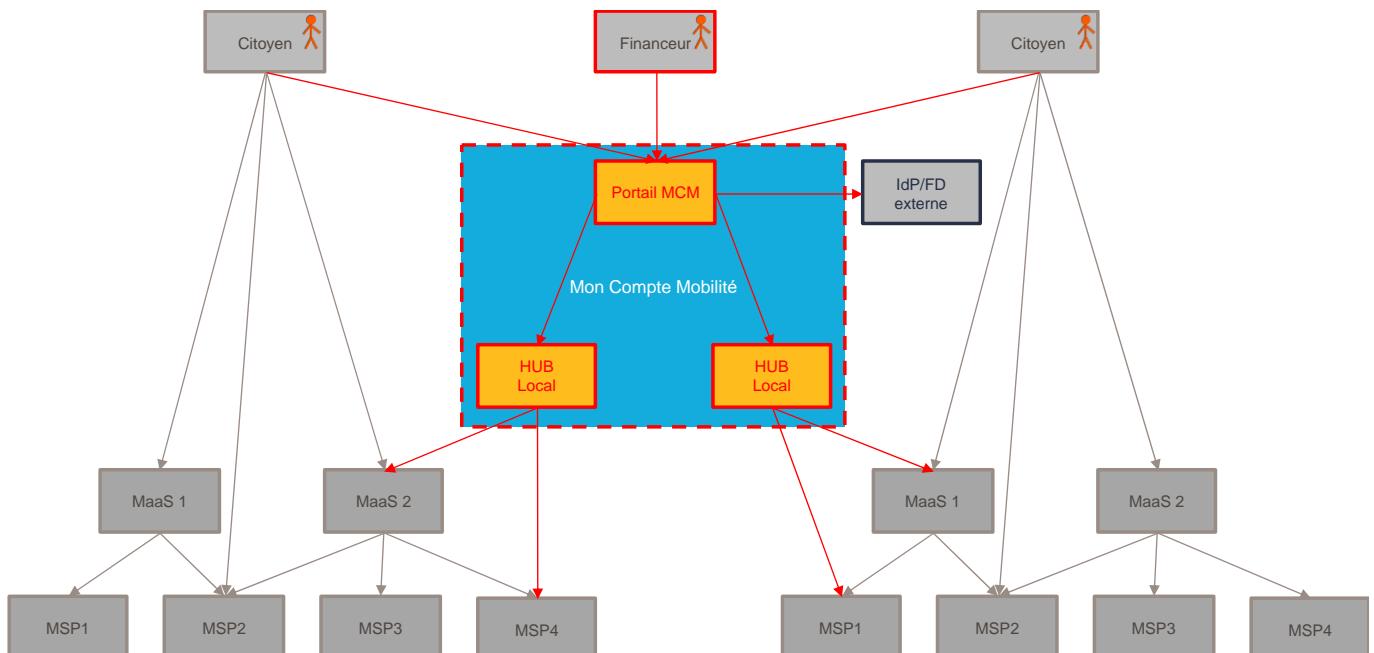


Figure 14 – HUB locaux

Le second axe de décomposition que nous avons retenu est fonctionnel. L'analyse des différentes fonctionnalités exposées par le système et les entités décrites précédemment nous permettent d'identifier des domaines de responsabilités distincts :

- La gestion des comptes et des identités. Ceci inclut aussi bien les citoyens que les collectivités et les entreprises, les personnes physiques que les systèmes tiers, leurs points de terminaison et les éventuels adaptateurs, les fournisseurs d'identités ou de données certifiées.

- La gestion des offres : offres de mobilité, dispositifs incitatifs.
- La gestion des droits de mobilité. Ce domaine couvre aussi bien les demandes d'affiliation, les portefeuilles de mobilité, la gestion des demandes d'octroi que les justificatifs associés.
- D'autres domaines annexes concernent les communications et le support technique aux utilisateurs.

Les communications inter domaines à l'intérieur du système seront assurées par des messages asynchrones via des mécanismes d'intégration.

Les communications depuis et vers les systèmes externes transiteront via des interfaces d'entrées/sorties définies, à l'aide de protocoles de transport standards et suivant des schémas publics, maintenus et versionnés (APIs).

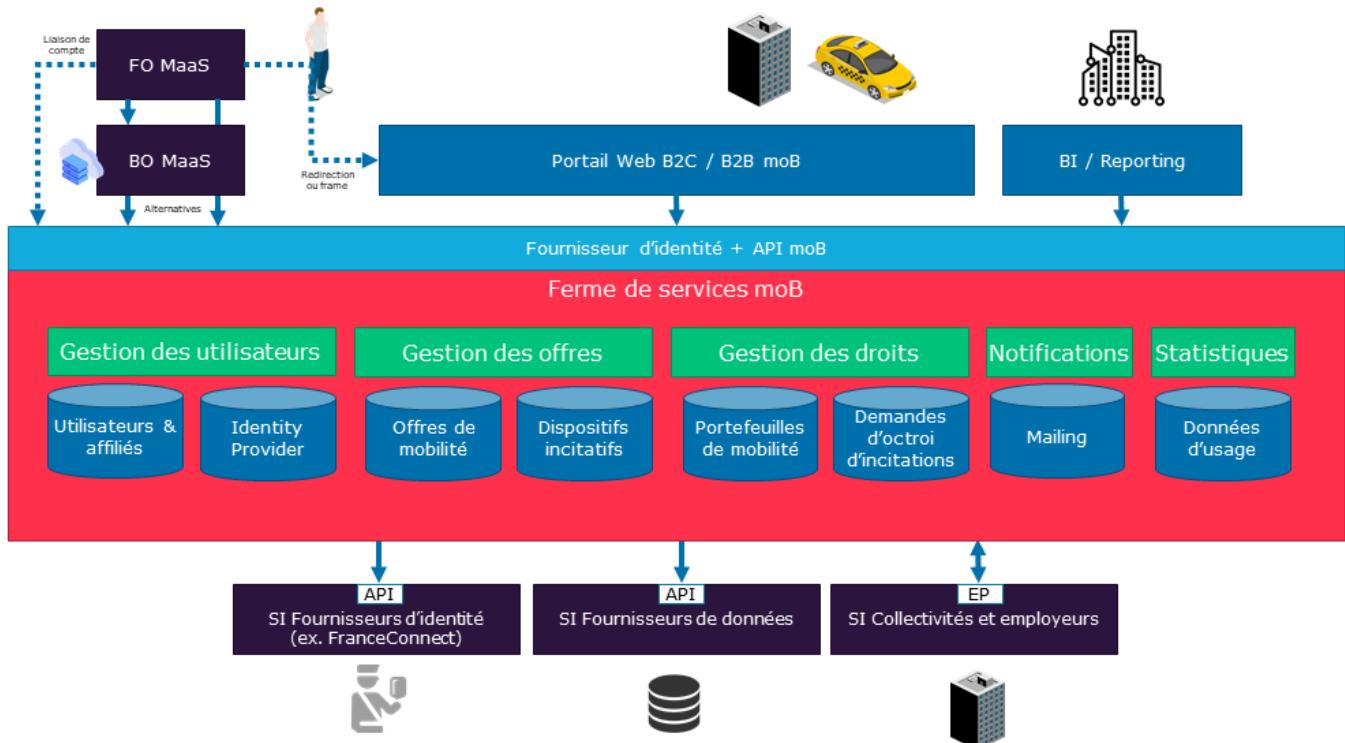


Figure 15 – Sous-systèmes logiques

4.3. Stockage et utilisation des données

Chaque domaine est responsable des données qui lui sont propres. Les entités ne sont définies que dans un seul domaine référentiel. Les autres domaines peuvent faire référence à une entité qu'ils ne possèdent pas par son identifiant technique, les attributs essentiels pouvant être répliqués à condition que la cohérence soit garantie.

Suivant la nature des données à persister, plusieurs types de stockages peuvent être envisagés : stockage structuré ou non, relationnel, orienté documents ou clés/valeurs.

4.4. Flux et cinématique

4.4.1. Vue d'ensemble

Le schéma qui suit illustre les flux entrants et sortants de moB. Les pastilles rouges indiquent la séquence des messages échangés. Afin d'être complets sémantiquement et de permettre une compréhension de bout en bout du processus, nous avons également capturé en gris les échanges intervenant en dehors de moB.

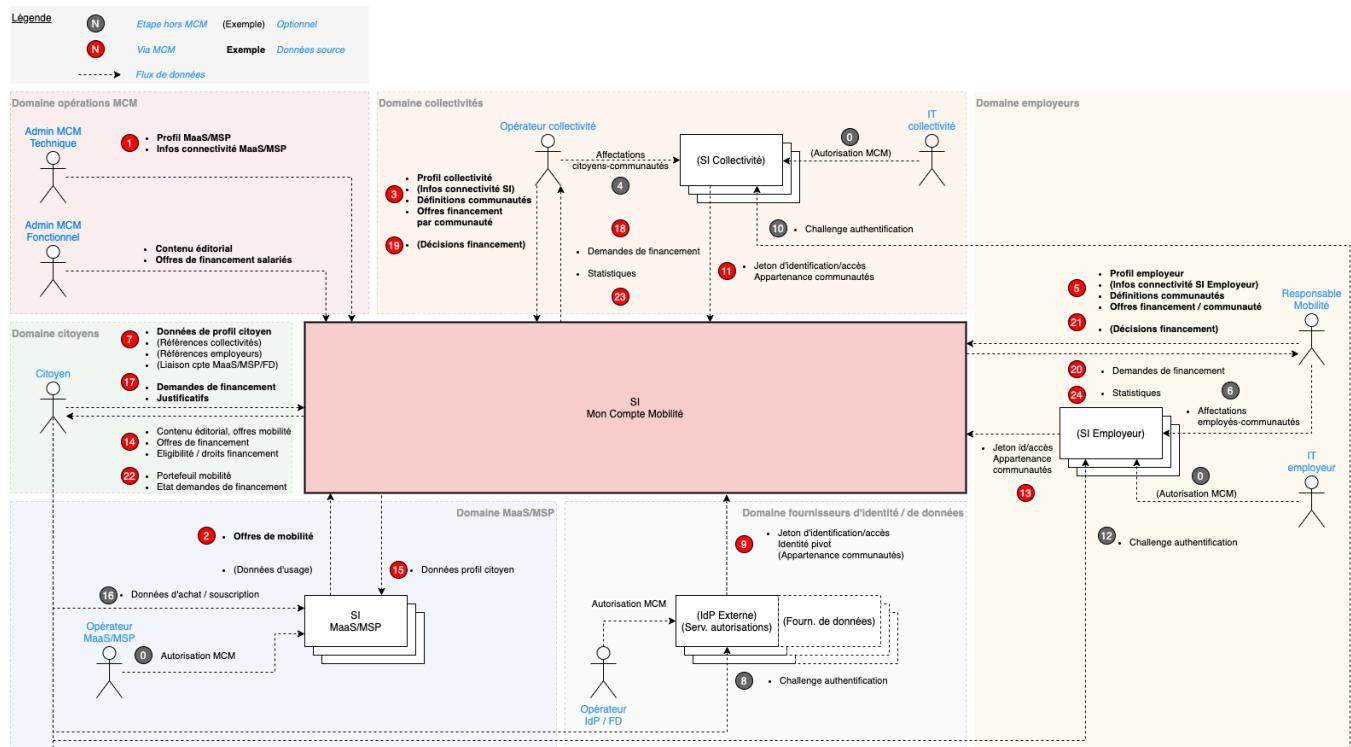


Figure 16 – Flux et cinématique – vue d'ensemble

Le diagramme peut être interprété de la façon suivante :

- Afin que le SI d'un MaaS/MSP, d'une collectivité ou d'une entreprise puisse être contacté par la plateforme Mon Compte Mobilité, un lien de confiance doit être créé. Un administrateur doit autoriser moB à contacter le SI. Il s'agit d'enregistrer l'URL et éventuellement l'adresse IP de Mon Compte Mobilité auprès du service. Puis, une clef secrète doit être générée par le service afin de permettre l'authentification de Mon Compte Mobilité.
- Un administrateur technique de Mon Compte Mobilité crée le compte du MaaS/MSP en renseignant les caractéristiques du point de terminaison technique. Ceci inclut le secret généré par le service distant pour authentifier Mon Compte Mobilité.
- Une fois le MaaS/MSP dûment enregistré, les offres de mobilité peuvent être transmises à Mon Compte Mobilité.
- Le personnel d'une collectivité ou un administrateur Mon Compte Mobilité réalise l'inscription de la collectivité. Outre le profil, les données de connectivité, les communautés et les dispositifs incitatifs peuvent être transmis.

4. En dehors de moB, l'opérateur doit s'assurer que les utilisateurs du SI de la collectivité soient effectivement associés aux communautés déclarées auprès de Mon Compte Mobilité.
5. Un mécanisme similaire à (3) est mis en œuvre pour inscrire une entreprise.
6. De même qu'en (4), en dehors de Mon Compte Mobilité, dans le système d'information de l'entreprise, un administrateur doit s'assurer de la cohérence des correspondances employés-communautés.
7. Aussitôt le service disponible, les MaaS/MSP et entreprises déclarés, les citoyens ont la possibilité de créer leurs comptes. C'est à ce moment qu'ils peuvent indiquer les collectivités et les entreprises auxquelles ils sont affiliés.
8. Au lieu de créer un compte ex-nihilo, le citoyen peut choisir de s'authentifier auprès d'un fournisseur d'identité externe comme FranceConnect.
9. Dans ce cas, Mon Compte Mobilité reçoit un jeton d'accès, un jeton d'identité/l'identité pivot de l'utilisateur. Des données concernant les communautés auxquelles il appartient peuvent éventuellement figurer dans la réponse.
10. Le citoyen ayant déclaré son rattachement à une collectivité, cette dernière disposant d'un SI accosté à Mon Compte Mobilité, une procédure d'authentification est déclenchée par moB.
11. A l'issue du défi d'authentification, Mon Compte Mobilité reçoit les jetons d'accès et d'identité émis par le SI de la collectivité.
12. De même qu'en (10), une procédure d'authentification est ensuite initiée afin de vérifier l'appartenance du citoyen au personnel de(s) l'entreprise choisie.
13. Comme en (11), Mon Compte Mobilité est notifié et reçoit des jetons en cas de succès.
14. Le citoyen parcourt le site à la découverte des offres de mobilité et des dispositifs incitatifs.
15. Il choisit de naviguer vers le site d'un fournisseur de mobilité. Il est redirigé par Mon Compte Mobilité vers le service requis. Les données du profil citoyen sont transmises au service avec le consentement de l'usager.
16. L'usager souscrit/consomme le service de mobilité. Cette transaction a lieu hors de Mon Compte Mobilité, directement auprès du fournisseur.
17. A l'issue de la transaction, le citoyen saisit une demande d'octroi d'incitation dans Mon Compte Mobilité. Il upload les justificatifs requis.
18. Si la demande concerne une collectivité, elle est transférée vers le service adéquat.
19. Une fois la demande instruite, la décision est retournée à Mon Compte Mobilité. Cette instruction peut être manuelle si aucun SI n'est accosté par exemple, ou automatique si le système tiers le permet.
20. Comme en (18), un processus similaire peut être déroulé dans le cas d'une demande instruite par une entreprise.
21. De même qu'en (19), la décision est transmise à Mon Compte Mobilité.
22. À tout moment, le citoyen peut suivre l'avancement de son dossier et consulter son portefeuille mobilité.
23. La collectivité peut consulter les statistiques d'usage et/ou exporter des données en vue d'une intégration et d'un traitement automatisé dans son propre SI.
24. Des fonctionnalités similaires sont offertes aux entreprises participant au programme.

4.4.2. Établissement du lien de confiance entre FranceConnect et moB

Préalablement à toute sollicitation de FranceConnect par moB, un lien de confiance devra être établi entre les 2 services. Cette opération n'est requise qu'une seule fois. Elle prend la forme d'un engagement contractuel entre les 2 opérateurs qui s'échangent les données suivantes :

- L'URL de moB est communiquée à FranceConnect via le [portail partenaires](#)
- FranceConnect communique à moB un identifiant unique, un secret ainsi que l'URL des points d'entrée permettant d'authentifier un visiteur, demander un jeton, demander le profil qui lui est associé aussi connue sous le nom d'identité pivot.

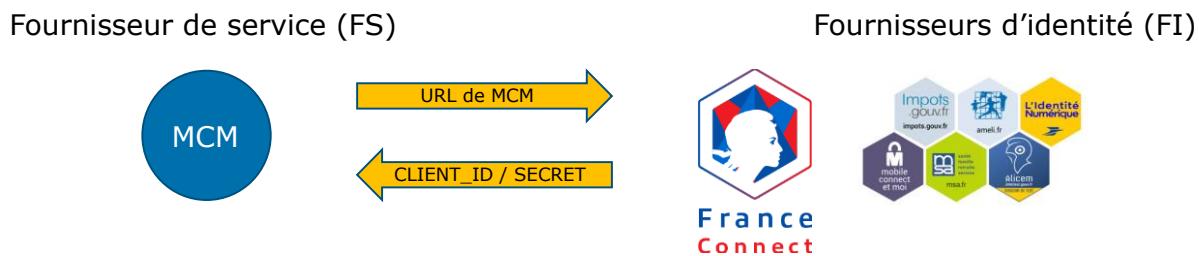


Figure 17 – Principe de l'habilitation FranceConnect

4.4.3. Authentification via FranceConnect

L'authentification via FranceConnect est possible grâce au protocole standard OAuth2 et au profil OpenID Connect.

FranceConnect n'est pas un fournisseur d'identité stricto sensu, mais propose une implémentation particulière de ce standard ouvert qui se distingue par 4 aspects :

1. L'utilisateur se voit offrir la possibilité de choisir l'un des 6 fournisseurs d'identité supportés.
2. Quel que soit le fournisseur d'identité sélectionné, FranceConnect redresse les données de l'identité pivot grâce au registre de l'INSEE.
3. FranceConnect garantit la stabilité de l'identifiant utilisateur même s'il change de fournisseur d'identité lors de connexions successives.
4. FranceConnect garantit la confidentialité de l'usager en :
 - obfusquant la nature de l'Identity Provider utilisé
 - générant des identifiants utilisateurs distincts pour chaque fournisseur de service afin d'empêcher les croisements de fichiers.

Cette première caractéristique — (1), le choix du fournisseur d'identité — se retrouve dans le diagramme de séquence ou de communication décrivant l'authentification via FranceConnect. Comme l'illustre le schéma ci-dessous, les interactions (3) et (4) distinguent le flux d'authentification FranceConnect — avec la sélection d'un fournisseur d'identité — de l'enchaînement classique spécifié par OAuth2/OpenID Connect.

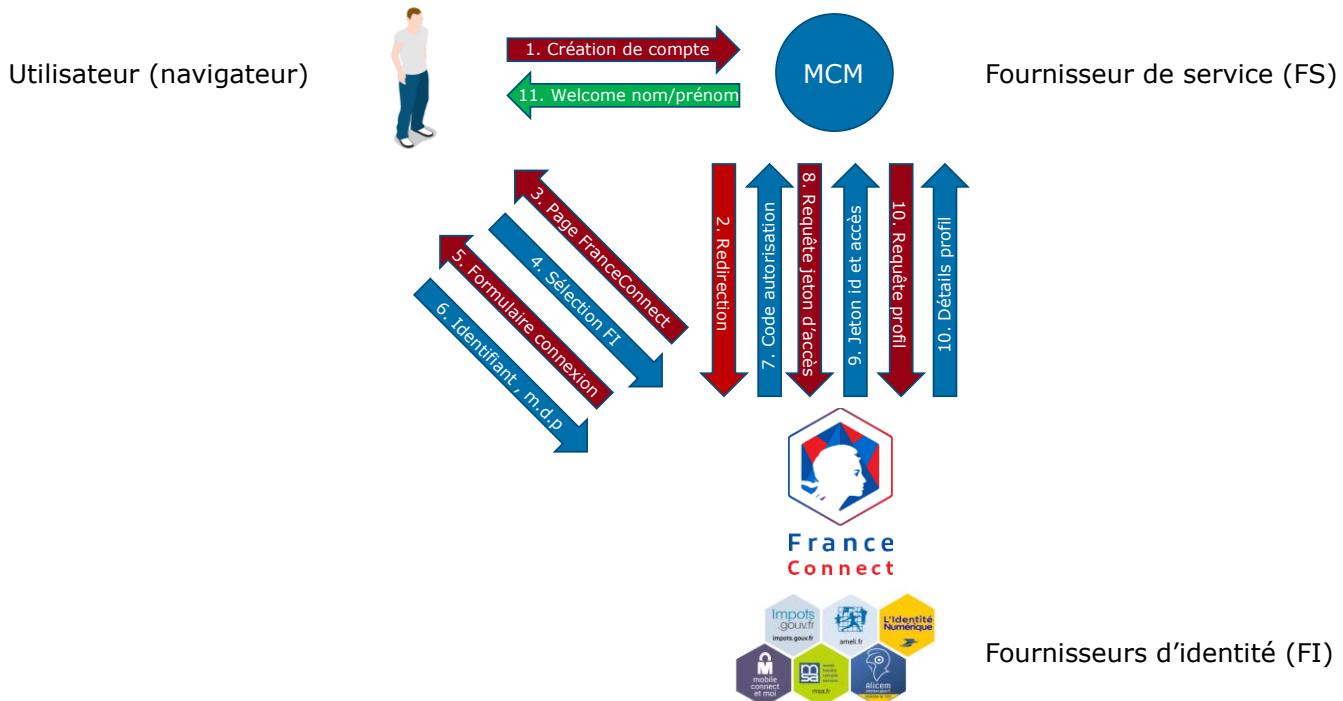


Figure 18 – Authentification via FranceConnect

4.4.4. Authentification financeur

Vérifier qu'un citoyen est salarié d'une entreprise ou affilié à un organisme consiste à réaliser un envoi d'email avec un lien d'affiliation unique contenant un jeton sécurisé.

Le citoyen clique sur le lien et valide de fait l'affiliation avec l'entreprise.

4.4.5. Autres APIs pour l'obtention de preuves

Nous avons passé en revue les APIs des services publics afin de déterminer celles dont pourrait bénéficier Mon Compte Mobilité pour l'obtention de preuves et de données certifiées.

Un processus d'habilitation est toujours requis préalablement à l'utilisation de ces APIs. Par ailleurs, la plupart des APIs sont FranceConnectées. Ceci implique qu'elles peuvent être invoquées uniquement si l'usager consent à être authentifié via FranceConnect.

Nous énumérons ci-dessous les données que nous pouvons obtenir à l'aide des 6 APIs identifiées.

Nom	Habilitation	FranceConnectée	Entrées	Sorties utiles	
FranceConnect	Oui	N/A	<ul style="list-style-type: none"> Données de connexion 	<ul style="list-style-type: none"> Identité pivot 	PMV
API Particulier	Oui	Non	<ul style="list-style-type: none"> Numéro fiscal, numéro d'avis d'imposition Numéro allocataire CAF, code postal 	<ul style="list-style-type: none"> Avis d'imposition Composition famille Adresse déclarée CAF Quotient familial 	
API Impôt Particulier	Oui	Oui	<ul style="list-style-type: none"> Année fiscale 	<ul style="list-style-type: none"> Revenu fiscal de référence Nombre de parts fiscales Adresse fiscale de taxation 	PMV
API CNAM Droits à Assurance Maladie	Oui	Oui	<ul style="list-style-type: none"> Plage de recherche (dates) 	<ul style="list-style-type: none"> Bénéficiaires 	
Justif'Adresse	?	?	<ul style="list-style-type: none"> ? 	<ul style="list-style-type: none"> Adresse connue des fournisseurs d'énergie affiliés 	
Registre de Preuves de Covoiturage	Oui	?	<ul style="list-style-type: none"> ? 	<ul style="list-style-type: none"> Certificat de covoiturage 	

Figure 19 – API FranceConnectées

5. Principes directeurs

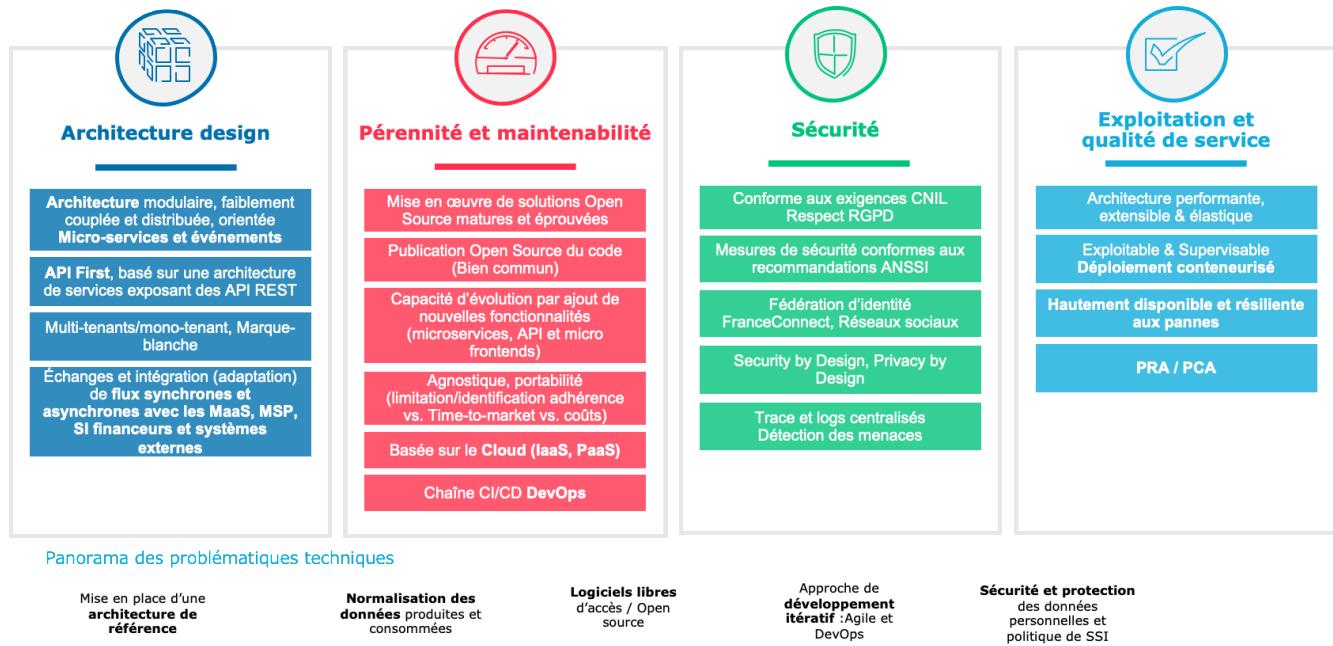


Figure 20 – Principes directeurs d'architecture

Architecture design

L'architecture moB est urbanisée, modulaire, faiblement couplée et distribuée.

Les modules implémentent des services métiers (micro-services) exposés sous la forme d'APIs REST proposant des contrats d'interface.

Les interfaces graphiques consomment directement les APIs REST en approche SPA (Single Page Application). Une approche modulaire permet de réaliser des interfaces composites (micro frontends).

L'architecture moB est conçue pour supporter les modes multi-tenants, mono-tenant et marque blanche.

Le sous-système gérant les échanges permet d'intégrer des sources et flux de données de manière évolutive et modulaire. Il supporte les flux synchrones et asynchrones et réalise les échanges avec les MaaS, MSP et SI financeurs.

Pérennité & Maintenabilité

L'architecture moB utilise des technologies et solutions Open Source matures et éprouvées.

L'architecture proposée, du fait de sa construction et sa modularité, offre des capacités d'évolution par ajout de nouvelles fonctionnalités dans les modules et par ajout / remplacement de modules.

Afin de maîtriser l'évolution du système dans le temps et d'assurer une gouvernance des APIs et des données (cycle de vie, catalogue, versioning, analyse impacts, ...), une gouvernance outillée est mise en œuvre.

L'architecture moB est hébergée dans le Cloud Azure et met en œuvre des ressources IaaS et PaaS.

Les choix de composants et de solutions s'attachent à être le plus agnostique possible et à faciliter la portabilité entre environnements d'hébergement.

L'architecture moB met en œuvre une chaîne CI/CD, en approche DevOps, permettant de réaliser l'intégration continue des composants, de mesurer la qualité, et d'automatiser la non-régression, les tests et le déploiement.

Sécurité

L'architecture moB met en œuvre les recommandations et exigences de la CNIL dans le respect de la GDPR (Privacy by Design).

Le système MCM intègre les exigences et contraintes de sécurité (Security by Design) et met en œuvre les principaux mécanismes et mesures de sécurité suivants :

- Chiffrement (HTTPS, SFTP, SSL/TLS) des flux échangés
- Cloisonnement et sécurisation des réseaux
- Mise en œuvre de groupes de sécurité
- Accès APIs protégé par API Gateway / Reverse proxy
- Contrôle d'intégrité (checksum) lors des échanges de fichiers
- Traces et logs centralisées
- Mise en œuvre et vérification des bonnes pratiques de la sécurité dans le code
- Vérification automatique (chaîne CI/CD) des vulnérabilités Top 10 OWASP
- Vérification automatique des vulnérabilités divulguées publiquement et contenues dans les dépendances des librairies des projets
- Gestion de l'identité et des accès des administrateurs techniques et les administrateurs fonctionnels par la mise en œuvre d'une solution d'IAM (Identity Access Manager) permettant la fédération des identités et le Web SSO
- Permissions d'accès basées sur RBAC (Role-Based Access Control)
- Sauvegarde / snapshot

Exploitation & Qualité de service

L'architecture du système MCM met en œuvre des solutions d'administration technique et fonctionnelle et des outils de supervision & monitoring permettant d'exploiter le système.

Les mécanismes de haute-disponibilité (composants redondés, multi-instances, répartition de charge, tolérance aux pannes), l'extensibilité et les performances des solutions proposées permettent de se conformer au niveau de qualité de service demandé et de garantir la résilience du système en conformité avec le PRA/PCA.

L'hébergement du système moB dans le Cloud Azure (IaaS et PaaS) couplé à une automatisation de la création des instances et des environnements (Infrastructure as Code), et à l'utilisation d'un orchestrateur de conteneurs permet d'offrir une extensibilité et une élasticité du système.

6. Architecture technique

6.1. Schéma de principe

Dans cette section, nous nous intéressons aux composants de la plateforme Mon Compte Mobilité. Dans un premier temps, nous ferons abstraction des choix technologiques, des implémentations et optimisations éventuelles en nous concentrant uniquement sur la fonction des sous-systèmes.

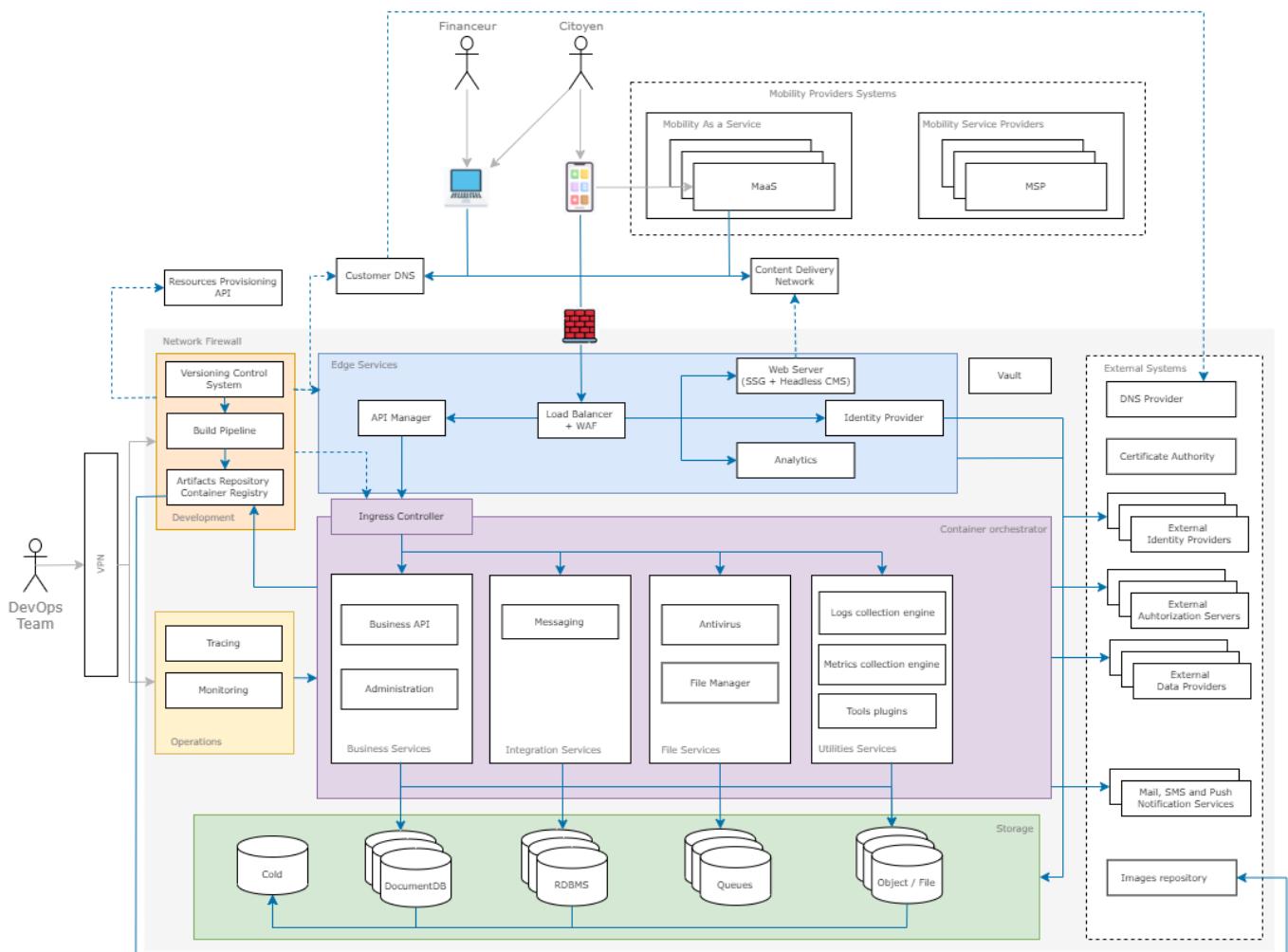


Figure 21 – Architecture technique – schéma de principe

Pour décrire le comportement du système, nous pouvons considérer 2 phases de son cycle de vie : la construction par l'équipe de développement et l'utilisation par les bénéficiaires du service.

L'ensemble des ressources de calcul est hébergé dans une infrastructure dont l'accès est contrôlé par un pare-feu. L'unique prérequis est que l'infrastructure supporte le provisionnement de ressources de façon programmatique via une API. Il peut aussi bien s'agir d'un cloud public que d'un cloud privé.

Les capacités de stockage sont également fournies sous la forme de services supportant divers types de bases de données : relationnelles ou non relationnelles.

La forge logicielle est hébergée au sein de cette infrastructure et s'exécute dans des machines virtuelles ou des conteneurs. Elle est composée d'un système de gestion de versions, d'un outil d'intégration et de déploiement continus, d'un dépôt de binaires et d'images.

La chaîne d'intégration/déploiement continu est en mesure d'invoquer un outil d'« infrastructure as code » qui automatise la construction des ressources telles que les réseaux, machines virtuelles, groupes de sécurité, les bases de données. L'outil d'IaC utilise pour cela l'API exposée par le gestionnaire de l'infrastructure.

La chaîne de déploiement continu est par conséquent en mesure de configurer aussi bien l'infrastructure que les environnements applicatifs.

Les identifiants requis pour accéder aux différentes ressources et services protégés sont stockées dans un outil de gestion de secrets / un coffre-fort.

Le firewall est configuré pour permettre les connexions à la forge uniquement aux employés de Capgemini affectés au projet MCM. Les développeurs devront s'authentifier à l'aide des mécanismes de sécurité fournis par Capgemini (authentification multi-facteurs).

En revanche, le pare-feu autorise les connexions entrantes sur les ports réservés à http (80) et/ou https (443) quelle que soit leur origine. C'est par ce canal que les requêtes provenant des utilisateurs finaux parviendront à Mon Compte Mobilité.

Quelle que soit la nature du périphérique utilisé par l'utilisateur, le navigateur commencera par résoudre le nom de domaine — par exemple *moncomptemobilité.fr* — auprès du serveur DNS et obtiendra l'adresse IP publique du réseau de distribution de contenu (CDN) ou de l'étage d'entrée de la plateforme. Cette dernière est constituée en premier lieu d'un proxy inverse assurant la fonction de répartiteur de charge et de pare-feu applicatif.

Seules les requêtes valides — exemptes de motifs suspects — seront routées vers les services applicatifs : serveur de contenu statique, fournisseur d'identité, etc.

Lors du premier accès à la page racine du site Mon Compte Mobilité, le CDN accédera au serveur de ressources statiques et mettra en cache les fichiers obtenus.

Le premier ensemble d'assets restitués au navigateur (index.html, fichiers JavaScript, feuilles de styles et images) permettront d'initialiser l'application web monopage.

L'utilisateur aura alors la possibilité de poursuivre sa navigation de façon anonyme ou de s'authentifier. Auquel cas, un défi d'authentification lui sera proposé par le fournisseur d'identité. En cas de succès, des jetons d'accès, d'identité et de rafraîchissement seront retournés à l'application.

Par la suite, le navigateur m'émettra plus que des appels d'APIs au backend de Mon Compte Mobilité en passant systématiquement le jeton d'accès en sa possession. Ces requêtes seront interceptées, sécurisées, auditées et routées par l'API Manager.

La logique métier côté backend est implémentée sous la forme de multiples conteneurs, selon le style d'architecture microservices. Ces conteneurs sont lancés, dimensionnés, surveillés par un orchestrateur qui s'assure de leur état de santé, les redémarre si nécessaire.

L'orchestrateur constitue également une plateforme facilitant le développement. En proposant une approche déclarative plutôt qu'impérative, il se substitue au développeur et détermine automatiquement les transitions nécessaires pour atteindre l'état cible configuré. Par ailleurs, il comporte un annuaire auprès duquel les services exposés par les conteneurs peuvent s'enregistrer afin qu'ils puissent être découverts par leurs clients. Enfin, le contrôleur d'entrée (ingress controller) exploite les informations de l'annuaire de services pour assurer la répartition de charge et permettre la mise en œuvre de stratégies de déploiement avancées comme le blue/green deployment ou les rolling updates.

Le trafic sortant vers les systèmes externes est contrôlé par le firewall.

Un point d'accès spécifique permet aux administrateurs de réaliser les opérations de surveillance et de maintenance du système.

6.2. Justification des choix d'architecture

Plusieurs facteurs ont été pris en compte afin de sélectionner les composants permettant d'implémenter cette architecture cible :

- La rapidité de mise en œuvre : le souhait de l'équipe projet est de valider la valeur de la proposition auprès des utilisateurs participant au pilote. Ce but peut être plus facilement atteint si l'effort de développement est concentré sur le fonctionnel plutôt que l'infrastructure technique. Par ailleurs, les coûts de réalisations sont inversement proportionnels à la vitesse.
- La maîtrise des coûts de licence : ces derniers constituent une incitation forte à favoriser les composants open source.
- Les coûts : le modèle de responsabilités partagées proposé par les fournisseurs de clouds permet de libérer l'équipe projet de certaines tâches récurrentes telles que les mises à jour. Inversement, en l'absence de contrat de maintenance, le choix de briques open source est susceptible d'augmenter l'effort de maintien en condition opérationnelle.
- Le vendor lock-in et l'impact sur la réversibilité : le choix d'un service managé doit être entouré de précautions car il implique un couplage à la plateforme cloud. Si l'interface dudit service respecte un standard supporté par plusieurs implantations tierces, alors une substitution un-pour-un est possible. En revanche, dans le cas d'une interface propriétaire un rework plus ou moins doit être provisionné afin de permettre la réversibilité. A ceci s'ajoute la difficulté potentielle à migrer les données. Ce risque existe même en présence d'interfaces normalisées : c'est le cas par exemple des services/composants gérant des secrets lorsque ceux-ci ne peuvent être exportés à des fins de migration.

En définitive, 3 stratégies sont possibles pour choisir les technologies :

1. Le tout managé qui offre l'avantage de la rapidité au détriment des coûts de licence et de réversibilité ;
2. Le tout open source qui contourne le problème des licences, facilite la réversibilité — pourvu que les modules choisis soient approuvés par le repreneur — mais augmente les coûts de construction et d'opérations ;
3. Une combinaison des deux stratégies précédentes : opter pour des services managés lorsqu'une ou plusieurs options open source interchangeables existent ; démarrer avec une brique open source lorsque la migration n'est pas triviale.

La stratégie 3 est celle retenue pour notre solution.

6.3. Architecture technique du PMV

Nous présentons ici l'architecture retenue. Nous préconisons de recourir aux services managés d'Azure pour la plupart des aspects à l'exception de :

- La forge logicielle : migrer d'Azure DevOps vers toute autre solution impliquerait une réécriture des scripts d'intégration et de déploiement. Par ailleurs, une partie des données d'historique serait perdue. Enfin, l'expérience développeur est supérieure dans le cas de la solution concurrente. La licence GitLab premium est celle utilisée dans le cadre de ce projet.
- Le fournisseur d'identité est accessible à travers des interfaces non standards, induisent un coût initial de mise en œuvre significatif — et par conséquent un risque de rework qu'il est

souhaitable d'atténuer — du fait de leur complexité, et embarquent des données difficiles à reprendre.

- Enfin, les briques d'intégration permettant l'interfaçage avec les MaaS et MSP.

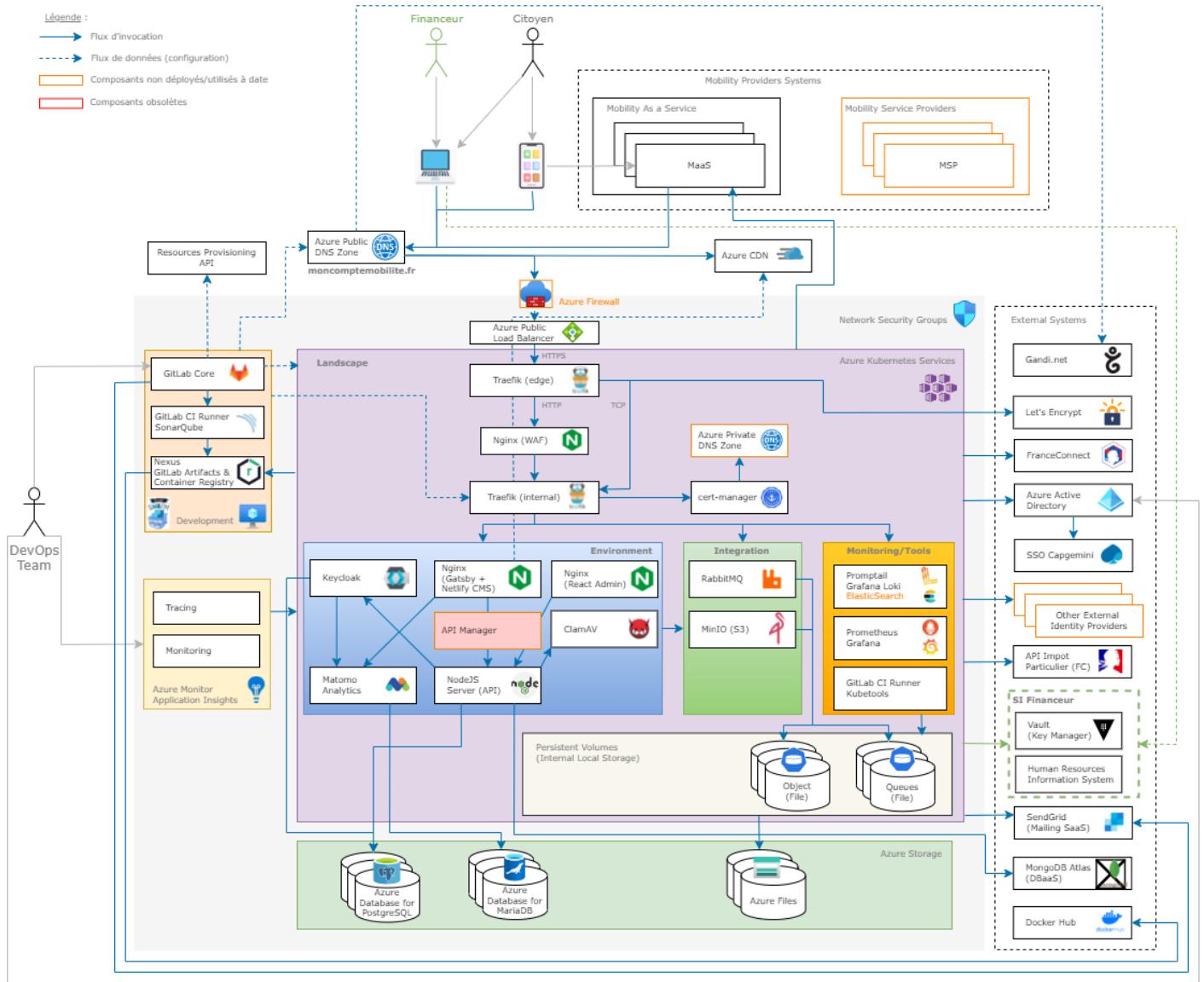


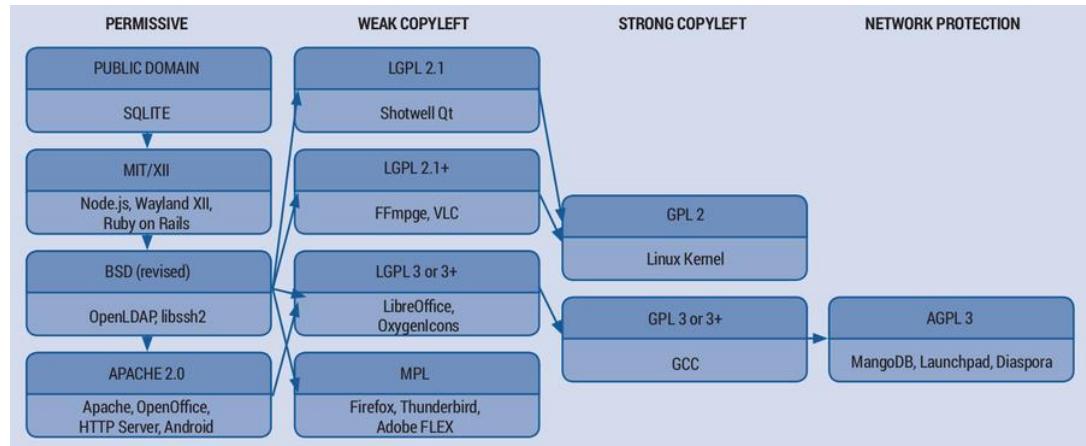
Figure 22 – Architecture technique – Solution retenue/enrichie pour le PMV

6.4. Licences open sources autorisées

Selon les objectifs de protection recherchés, il existe plusieurs classes de licences largement répandues et conduisant à des obligations diverses :

- Les licences permissives autorisent l'édition d'une œuvre dérivée sous une autre licence, même propriétaire, restreignant les droits de ses utilisateurs. Les plus connues sont les licences MIT et BSD.
- Les licences « copyleft » ou « gauche d'auteur », faible et fort : à l'instar de la licence GPL, elles impliquent une obligation de publication du code des œuvres dérivées sous une licence similaire, l'intention étant de garantir le partage de la connaissance comme bien commun.

- Et celles du type « network protection » : elles prennent en compte les interactions avec un produit à travers un réseau. C'est le cas notamment de la licence Affero GPL qui est du type copyleft. Elle a pour but d'obliger les services accessibles par le réseau de publier leur code source.



Source https://en.wikipedia.org/wiki/Free_software_license

Par ailleurs, l'Etat définit les licences qui sont applicables aux codes sources des logiciels publiés par l'administration sur le site [data.gouv.fr](https://www.data.gouv.fr/fr/licences) : <https://www.data.gouv.fr/fr/licences>

Licences permissives	identifiant SPDX
Apache License 2.0	Apache-2.0
BSD 2-Clause "Simplified" License	BSD-2-Clause
BSD 3-Clause "New" or "Revised" License	BSD-3-Clause
CeCILL-B Free Software License Agreement	CECILL-B
MIT License	MIT

Licences avec obligation de réciprocité	identifiant SPDX
CeCILL Free Software License Agreement v2.1	CECILL-2.1
CeCILL-C Free Software License Agreement	CECILL-C
GNU General Public License v3.0 or later	GPL-3.0-or-later
GNU Lesser General Public License v3.0 or later	LGPL-3.0-or-later
GNU Affero General Public License v3.0 or later	AGPL-3.0-or-later
Mozilla Public License 2.0	MPL-2.0

La licence **CeCILL-B** utilisée pour le projet moB est très proche de la licence Apache 2.0 mais appliquée à la législation française, elle est plus récente et donc beaucoup moins répandue. La principale différence entre ces deux licences est dans l'obligation forte de citation qui se trouve dans CeCILL-B (article 5.3.4).

- La variante **CeCILL-B** utilisée en mai pour la publication de MCM Historique permet d'ajouter l'**obligation de citer MCM** qui reste importante, notamment pour **conserver la légitimité du projet dans les éventuelles reprises du projet** (par ex. cela permet d'éviter la création d'un 2^{ème} MCM sans évoquer le 1^{er}).
- La variante **CeCILL-C** ajoute une **obligation de réciprocité** et va donc plus loin, car elle **oblige les contributeurs à partager leurs modifications à la communauté**. On pourrait souhaiter cela pour les travaux de standardisation des MaaS, mais cela peut également être un frein.

Ainsi, toute personne (physique/morale) réutilisant le logiciel moB doit mentionner ce dernier et s'il le redistribue à un tiers, il doit faire en sorte que ce tiers mentionne également le logiciel moB.

Cette traçabilité importante pour le projet est absente avec la licence Apache.

Dans la mesure où moB possède une visée nationale, le code source est publié sous l'une des licences CeCILL-B ou CeCILL-2.1/CeCILL-C qui sont des transpositions en droit Français des licences BSD et GPL/LGPL respectivement.

6.5. Composants logiciels

Le tableau ci-dessous précise les composants et versions logicielles utilisés dans le cadre du projet moB.

Notez bien que les composants listés ci-dessous se répartissent en 2 catégories :

- Ceux qui sont déployés avec l'application ;
- Les composants technologiques qui sont mis en œuvre uniquement pendant la phase de construction ou de test par l'équipe de développement.

Composant	Solution	Version	Éditeur	Licence / Souscription	Lien
Système d'exploitation serveur	Ubuntu	20.04	Canonical	Multiples, principalement GPL	https://www.ubuntu.com/
Conteneurs	Docker	19.03.8	Docker	Apache License 2.0	https://www.docker.com
Orchestrateur de conteneurs	Azure Kubernetes Services	1.19.11	Google	Apache License 2.0	https://kubernetes.io/
Proxy Inverse / Load Balancer	Traefik	2.6.x	Traefik Labs	MIT License	https://doc.traefik.io/traefik/
Proxy Inverse / Pare-feu Web	Nginx	1.21.6	NGINX, Inc. Sysoev	BSD 2-clauses	https://www.nginx.com/
Gestion des certificats	Cert-Manager	1.4.0	Cert Manager	Apache License 2.0	https://cert-manager.io/
Authorité de certification	Let's Encrypt	-	Internet Security Research Group (ISRG)		https://letsencrypt.org/

Environnement d'exécution JavaScript	Node.js Loopback 4	16.14.2-alpine	-	MIT License	https://nodejs.org/ https://loopback.io/doc/en/lb4/index.html
Générateur de sites statiques	GatsbyJS	4.4.0	Gatsby	MIT License	https://www.gatsbyjs.com/
Gestion de contenu orienté git	NetlifyCMS	2.10	Netlify	MIT License	https://www.netlifycms.org/
IHM Web	ReactJS	17.0.2	Facebook	MIT License	https://reactjs.org
Librairie de test JavaScript	Jest	26.0.22	Facebook	MIT License	https://github.com/facebook/jest
Librairie de tests automatisés end-to-end	Cypress	9.5	Cypress.io	MIT License	https://docs.cypress.io
Système de gestion de bases de données	PostgreSQL	13.6	PostgreSQL	PostgreSQL License	https://www.postgresql.org
Base de données documents NoSQL	MongoDB Atlas		MongoDB, Inc.	MongoDB, Inc.'s	https://www.mongodb.com/fr-fr/atlas/database
Bus de messages	RabbitMQ	3.9.15	Pivotal Software	Mozilla Public License	https://www.rabbitmq.com/
Stockage d'objets hautes performances	MinIO	RELEASE.2021-09-24T00-24-24Z	MinIO, Inc	GNU Affero GPL v3.0	https://min.io/
Supervision & Monitoring	Prometheus	1.12.2	Prometheus	Apache License 2.0	https://prometheus.io
Plugin Supervision & Monitoring	Plugin Prometheus Node Exporter	1.0.0-rc.0	Prometheus	Apache License 2.0	https://github.com/prometheus/node_exporter
Plugin Supervision & Monitoring	Plugin Prometheus JMX Exporter	-	Prometheus	Apache License 2.0	https://github.com/prometheus/jmx_exporter
Dashboard Supervision & Monitoring	Matomo Analytics	4.8.0	Matomo	GNU GPL v3	https://fr.matomo.org/
Dashboard Supervision & Monitoring	Grafana	8.0.3	Grafana Labs	Apache License 2.0	https://grafana.com
Centralisation des logs	Grafana Loki	8.0.3	Grafana Labs	Apache License 2.0	https://grafana.com/oss/loki/

Agent de gestion des logs	Promptail	0.17.2	Grafana Labs	Apache License 2.0	https://grafana.com/docs/lokii/latest/clients/promtail/
Antivirus/Antimalware toolkit	ClamAV	ClamAV stable 0.10x.x	ClamAV	GPL-2.0-only	https://www.clamav.net/
IAM	Keycloak	16.1.1	JBoss Red Hat	Apache License 2.0	https://www.keycloak.org
Envoi de mails	SendGrid	Essential s 40K	Isaac Saldana, Jose Lopez, Tim Jenkins		https://sendgrid.com/
Versionning code	GitLab Premium	14.x	GitLab	Commercial License	https://gitlab.com/gitlab-org/gitlab
Gestionnaire dépôts objets binaires	Nexus Repository OSS	3.x (3.38.1-01)	Sonatype	Eclipse Public License 1.0	https://github.com/sonatype-nexus-community
Qualimétrie	Sonarqube	8.5.x	SonarSource	LGPL	https://www.sonarqube.org/
Gestionnaire de paquets Kubernetes	Helm	3.9.0	-	Apache License 2.0	https://helm.sh/
Outil (CLI) de control de clusters Kubernetes	kubectl	V1.24.0 Dernière stable	Kubernetes	Apache License 2.0	https://kubernetes.io/fr/docs/reference/kubectl/overview/
Infrastructure as Code	Terraform	0.12.24	HashiCorp	Mozilla Public License v2.0	https://www.hashicorp.com/products/terraform
Sauvegarde / restauration	Azure Backup	-	Azure		https://learn.microsoft.com/fr-fr/azure/backup/backup-overview
Ordonnanceur	Loopback CRON	2.4.0		MIT License	https://loopback.io/doc/en/lb4/Running-cron-jobs.html
Gestionnaire de clés de chiffrement	Vault	1.10.1	HashiCorp	Mozilla Public License v2.0	https://www.hashicorp.com/products/vault

6.6. Provisionnement des ressources dans Azure

Par plateforme, nous entendons un groupe de ressources machine, réseau et stockage isolé pouvant accueillir des piles logicielles. Des conditions d'accès distinctes peuvent s'appliquer aux plateformes.

Un environnement s'exécute au sein d'une plateforme. Il est en compétition avec les autres environnements de la même plateforme pour l'accès aux ressources. Toutefois, les environnements n'interfèrent pas entre eux.

Au sein de chaque environnement, des tiers peuvent être distingués : tiers web, logique métier et données. Le trafic réseau interne à l'environnement devrait idéalement faire l'objet de restrictions afin de forcer l'application des bonnes pratiques et limiter les risques de vulnérabilité.

Chaque environnement peut donner lieu à des déploiements successifs, chaque déploiement contenant une combinaison différente de versions de ses composants. La conservation de l'historique des déploiements et des binaires correspondants, la transparence sur leurs contenus/versions et la traçabilité jusqu'aux commits sont des qualités opérationnelles déterminantes pendant les phases de mise au point et de production.

Afin de répondre aux objectifs de sécurité et favoriser la lisibilité des rapports d'utilisation/factures des services Azure, il est souhaitable de ségréguer les ressources et le trafic réseau :

- Vis-à-vis des autres projets ;
- Entre les plateformes de développement et celles en production ;
- Entre environnements d'une même plateforme ;
- Entre les couches d'un même environnement.

Ces séparations peuvent être mises en œuvre grâce aux concepts supportés par Azure : les souscriptions, réseaux virtuels, groupes de sécurité et firewalls.

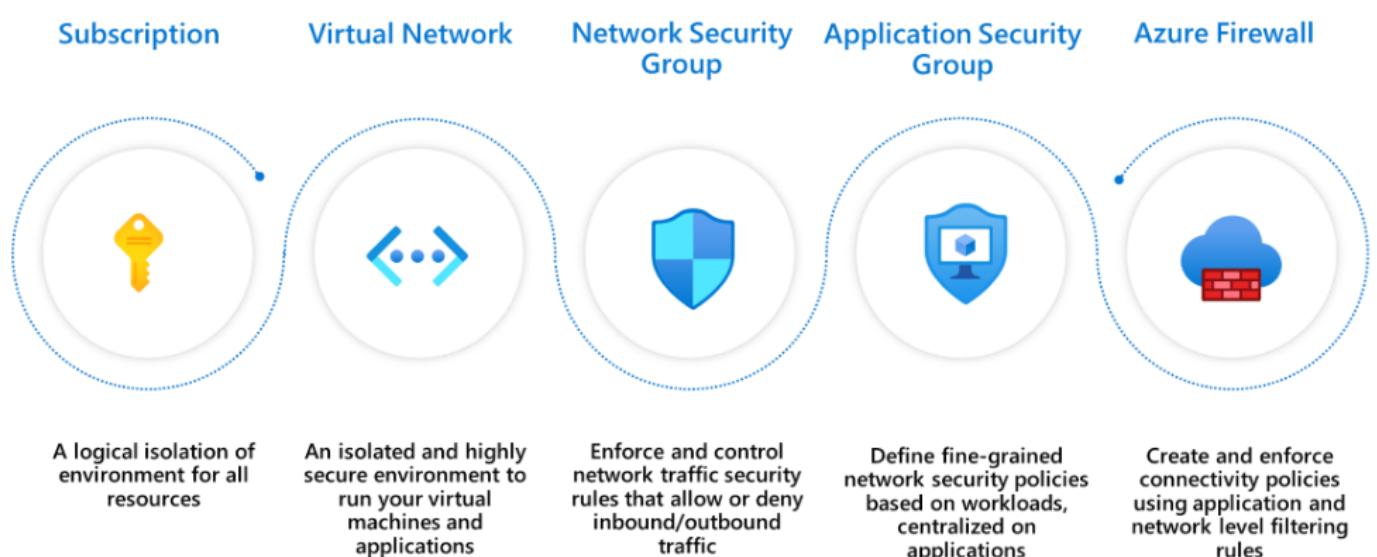


Figure 23 – Options de segmentation du trafic réseau dans Azure

Source : <https://docs.microsoft.com/fr-fr/.../network-level-segmentation>

6.7. Schéma réseau

En termes de topologie réseau :

- Chaque plateforme disposerait de son propre VNet.
- Le VNet associé à la plateforme des services partagés serait appairé à celui de toutes les autres plateformes, selon le modèle Hub & Spoke.
- Les Vnet des plateformes hors services partagés ne seront pas appairés entre eux.
- Au sein de la plateforme, et pour chaque environnement, des subnets seraient réservés pour les conteneurs de chaque tiers.

L'application des principes exposés à travers les sections précédentes conduirait à l'implémentation ci-dessous :

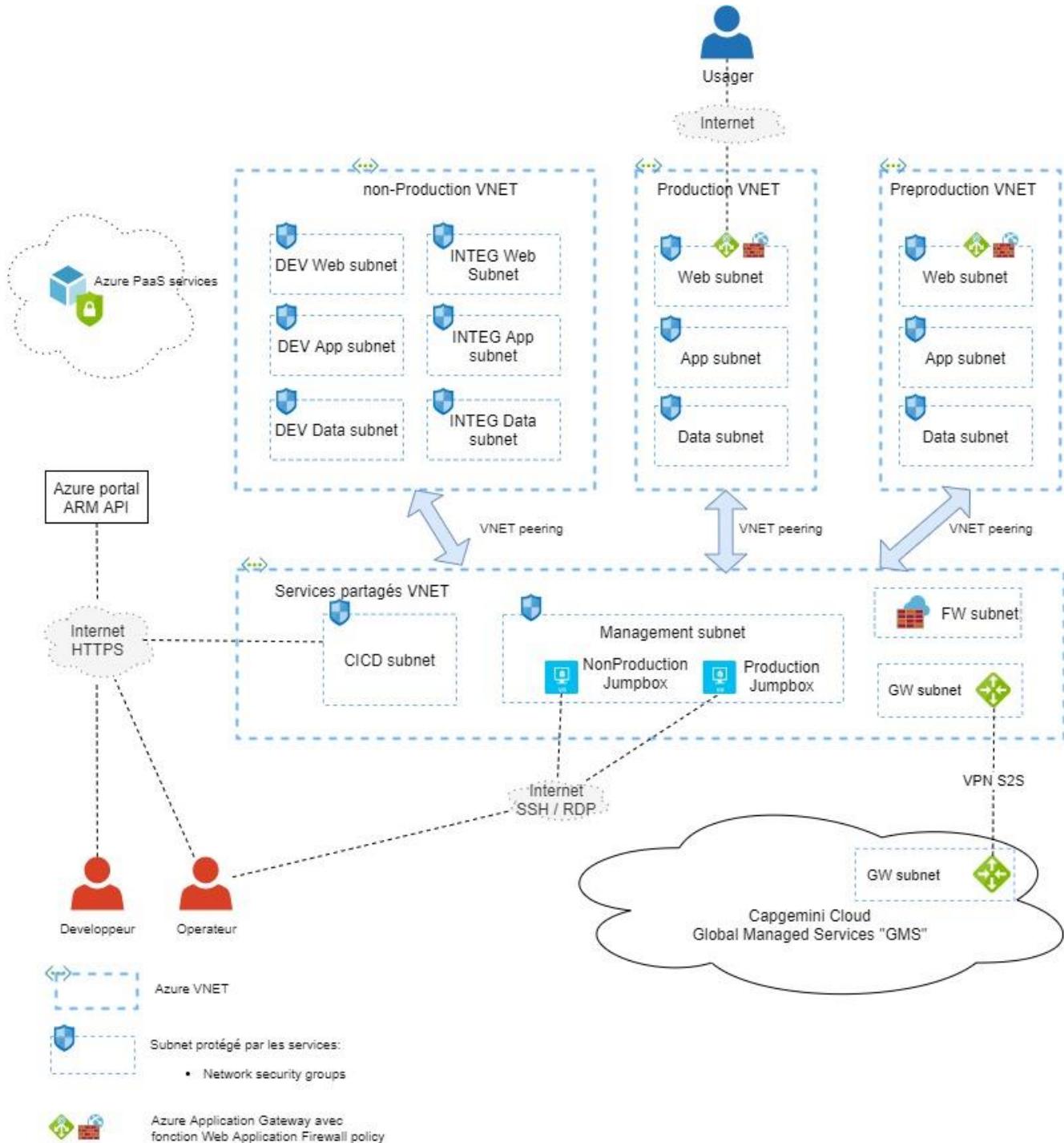


Figure 24 – Options de segmentation du trafic réseau dans Azure

Considérations :

- La connectivité entre VNet Peering n'est pas transitive. Le VNET de non-production n'est donc pas routable sur le VNET de production
- L'accès aux ressources PaaS backend (ex. DBaaS) doivent s'effectuer via des private links (gratuit) ou private endpoints (payant, \$0.01 par GB entrant/sortant).

6.8. Plateformes et environnements

Nous préconisons de distinguer les plateformes de non-production de celles dédiées à la production car elles devraient être opérées par des équipes distinctes.

Nous recommandons par conséquent les plateformes suivantes :

1 infrastructure Cloud pour héberger les ressources informatiques nécessaires au projet, en provisionner rapidement de nouvelles et bénéficier de services avancés :

- 1 plateforme de **développement** opérée par l'équipe de développement : elle contiendrait tous les environnements de développement, d'intégration, de validation.
- 1 plateforme de **préproduction** opérée par l'équipe infrastructure : elle contiendrait un ou plusieurs environnements destinés à des tests partenaires, de performance ou de bascule.
- 1 plateforme de **production** opérée par l'équipe infrastructure : elle ne contiendrait qu'un seul environnement accessible au public.
- 1 plateforme de **build et d'intégration continue CI/CD** permettant d'optimiser la chaîne de construction et de déploiement de l'infrastructure et des développements logiciels sur les différents environnements.

La répartition des plateformes dans les souscriptions Azure serait la suivante, chaque plateforme bénéficierait de sa propre souscription :

- Toutes les plateformes non-production (**développement** + testing) seraient affectées à une seule et même souscription.
- Les plateformes de **préproduction** et production partageraient une seconde souscription.
- La plateforme de **build et d'intégration continue CI/CD** serait isolée dans une 3^{ème} souscription.

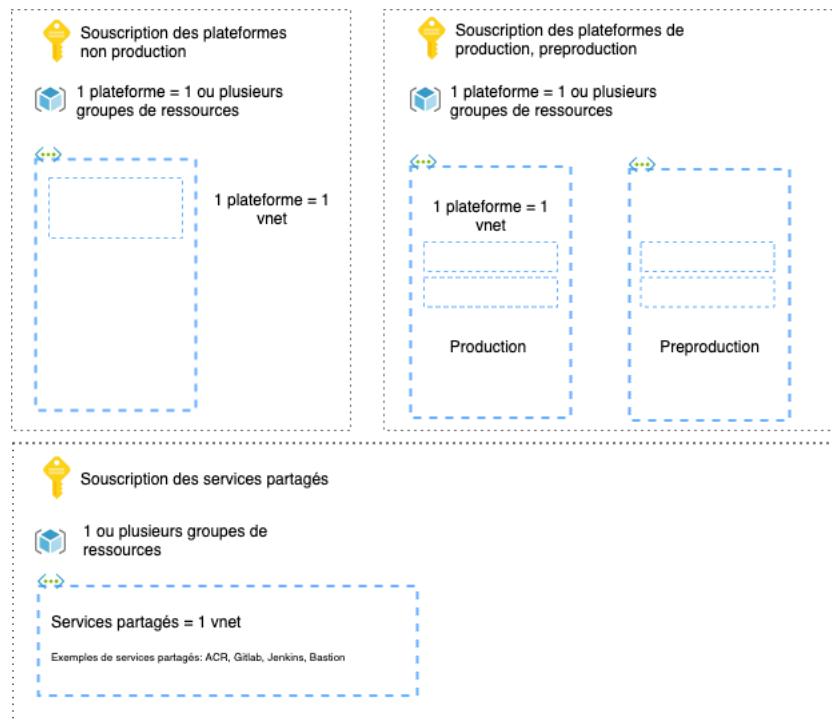


Figure 25 – Organisation des ressources dans Azure

Le tableau ci-dessous détaille les environnements techniques ainsi que les souscriptions dans le cloud Azure :

Landscape	Souscription Azure	Suffixe DNS	Résumé / Commentaires / Usage
CI / CD	SS- MCM-shared	*. cicd .moncomptemobilite.fr	<p>Ressources « Forge » partagées sur tout le programme MCM.</p> <p>Les pipelines de chaque projet GitLab permettent de déployer sur les landscapes preview/testing au moyen de ces ressources.</p> <p>1 cluster Docker Swarm constitué de :</p> <ul style="list-style-type: none"> • 1 VM GitLab Premium + Nexus • 1 VM Sonarqube
DEV	SS-MCM-developpement	*. preview .moncomptemobilite.fr *. testing .moncomptemobilite.fr	<p>1 cluster Azure Kubernetes de DEV global permettant d'héberger :</p> <ul style="list-style-type: none"> • 1 instance MOB master.preview basée sur la branche master du dépôt MOB. Cette instance est redéployée à chaque merge/commit, les données sont potentiellement rechargées à chaque fois. • 1 instance MOB.preview par branche / US Ces instances ont une durée de vie limitée. • 1 instance MOB.testing basée sur une Release Candidate GitLab. Cette instance est stable et s'appuie sur des BDD managées Azure. Les données ne sont jamais écrasées, seul le delta de version RC est pris en charge. C'est le dernier environnement avant livraison aux équipes OPS.
PREPROD	SS- MCM-production	*. preprod .moncomptemobilite.fr	<p>1 cluster Azure Kubernetes de préprod permettant d'héberger 1 instance MOB.preprod</p> <ul style="list-style-type: none"> • A destination des partenaires moB afin de valider l'intégration des évolutions du produit
PROD		*.moncomptemobilite.fr	1 cluster Azure Kubernetes de prod permettant d'héberger 1 instance MOB

7. Sécurité

7.1. Gestion des identités, identification & authentification

7.1.1. Acteurs humains

Catégorie utilisateur	Authentification
Citoyen / Usager	2 possibilités : <ul style="list-style-type: none"> (Obligatoire) Authentification gérée par moB : création d'un compte utilisateur (Optionnel) Authentification déléguée à France Connect
Administration fonctionnel	Accès internet SSL/TLS Accès via user/password
Administrateur technique	Accès VPN SSL/TLS + Bastion Gestion comptes administrateur via console d'administration Super utilisateur : accès via user/password Administrateur : accès via AK (Access Key) / SK (Secret Key) Gestion authentification et autorisation Web SSO (IAM) sur les ressources : <ul style="list-style-type: none"> Logging
Superviseur	Accès VPN SSL/TLS + Bastion Gestion authentification et autorisation Web SSO (IAM) sur les ressources : <ul style="list-style-type: none"> Logging Monitoring & Supervision
Développeur	Accès internet SSL/TLS

L'utilisateur (Citoyen) aura dans tous les cas 2 choix :

- Se connecter au service moB (et donc créer son compte) via FranceConnect** en utilisant ses identifiants AMELI ou Impôts par exemple ; dans ce cas, les données pivot du citoyen seront renvoyés à moB (Adresse mail, Nom, Prénom, Date de naissance...). Libre à lui par la suite de se connecter via FranceConnect (de manière directe sans avoir à introduire ses identifiants MCM) ou via ses identifiants MCM (adresse mail & mot de passe MCM).
- Se connecter au service moB (et donc créer son compte) via moB** en introduisant toutes ses informations d'identité manuellement et toujours en créant un mot de passe associé.
 - Dans le cas où l'utilisateur ne peut plus se connecter via FranceConnect (car oublie d'authentifiants AMELI ou Impôts...), il pourra utiliser ses identifiants moB.
 - Dans le cas où il oublie son mot de passe moB alors moB l'accompagnera dans la récupération ou la création d'un nouveau mot de passe.

7.1.2. Applications clientes

Catégorie utilisateur	Authentification
Maas / MSP / Financeurs	Accès internet SSL/TLS Gestion comptes via le gestionnaire d'identités (clientId / clientSecret) Gestion authentification et autorisation Web SSO (IAM) sur les ressources : <ul style="list-style-type: none"> • Logging • Monitoring & Supervision

7.2. Certificats serveurs et nom de domaine

Les certificats serveur utilisés sont obtenus auprès de l'autorité Let's Encrypt : crt.sh/_moncomptemobilite.fr

7.3. Autorisation et contrôle d'accès

Les permissions d'accès sont basées sur RBAC (Role-Based Access Control) et ACL (Access Control List).

7.4. Intégrité

L'intégrité des échanges est assurée par les protocoles HTTPS, SSL/TLS.

L'intégrité des fichiers échangés est assurée par un chiffrement hybride (symétrique + asymétrique).

7.5. Confidentialité

7.5.1. Flux / données échangées

Tous les échanges externes sont chiffrés en utilisant SSL/TLS, HTTPS.

L'accès aux APIs JSON / HTTPS est sécurisé par un Token JWT.

7.5.2. Données stockées

Les données sensibles stockées dans la base de données PostgreSQL sont stockées chiffrées (TDE : Transparent Data Encryption).

Les pièces justificatives du citoyen stockées dans le service S3 (MinIO) sont stockées chiffrées via un chiffrement hybride (chiffrement symétrique + asymétrique) ; chiffrement des pièces justificatives à l'aide d'une clé symétrique générée aléatoirement pour chaque demande d'aide effectuée par le citoyen, puis, cette clé symétrique est chiffrée à son tour à l'aide de la clé publique fournie par le financeur.

7.6. Traçabilité / Journalisation

La suite Grafana est utilisée pour collecter et centraliser les logs.

La collecte se fait via Promtail, qui les envoie à la fois sur Azure Logs Analytics et Grafana Loki.

Grafana Loki sert à la journalisation des logs, quelques tableaux de bord sont initialisés actuellement et stockées dans un volume à persister. Une rotation des logs est configurable.

Les logs sont tracés dans Azure Logs Analytics (possibilité de créer des tableaux de bord).

7.6.1. Logs techniques et applicatives

Les données concernant les logs techniques et applicatives seront journalisées. La durée de rétention reste à définir (durée courte).

7.6.2. Logs administrateurs techniques et fonctionnels

Tous les accès et actions (CRUD) réalisés par les administrateurs techniques et fonctionnels dans le système seront loguées. La durée de rétention reste à définir (durée longue correspondant à la période légale).

7.7. Imputabilité et non répudiation

L'imputabilité se base sur les mécanismes de journalisation mis en œuvre.

Le besoin de gérer la non-répudiation n'a pas été identifié comme exigence ; aucune mesure n'est mise en place.

7.8. Anonymisation & Pseudonymisation des données

Par conception, les données personnelles sont séparées des données d'usage. Des identifiants techniques non signifiants fonctionnellement sont utilisés pour en permettre la jointure.

Notamment, les données utilisées pour les statistiques se basent sur les identifiants techniques et ne nécessitent pas de processus d'anonymisation et/ou de pseudonymisation.

7.9. GDPR

À la demande du citoyen / usager, le système moB permet :

- De consulter les données ;
- De demander la suppression des données du système moB

7.10. Sauvegarde / restauration

Les logs techniques et applicatives sont sauvegardés. La durée de rétention des sauvegardes est paramétrable et reste à préciser.

La stratégie de sauvegarde est adressée au niveau applicatif :

- dump des bases de données avec les outils natifs des solutions (PostgreSQL)
- fonctionnalité de snapshots disponible nativement et instantanée
- utilisation du service de stockage objet pour archiver des données

Les snapshots permettent au CSP de pouvoir récupérer les données en cas de désastre (le cas échéant).

NB : Les sauvegardes sont stockées chiffrées.

7.11. Purge

Les données des souscriptions (quel que soit leur état) sont conservées 3 ans dans le système. Passé ce délai, elles sont purgées.

Les comptes inactifs depuis 2 années sont purgés.

7.12. Archivage

Pour répondre aux exigences juridiques et légales, les logs des accès des administrateurs (techniques et fonctionnels) sont sauvegardés et archivés. La durée de rétention des archives n'est pas précisée.

7.13. Anti-virus / anti-malware

Un sas de décontamination des pièces jointes et justificatifs a été mis en œuvre. Il permet d'analyser les fichiers afin de s'assurer qu'ils ne soient pas vérolés.

Une brique Antivirus a été intégré en utilisant l'outil **ClamAV**, qui répond bien au besoin. Cette brique est accessible par l'API pour scanner les pièces justificatives.

La brique Antivirus est installée dans le réseau interne pour des raisons de sécurité. Ce service prend en entrée le fichier à scanner et renvoie en sortie :

- Un champ isInfected = true ou false
- Un fichier scanné renvoyé ou détruit

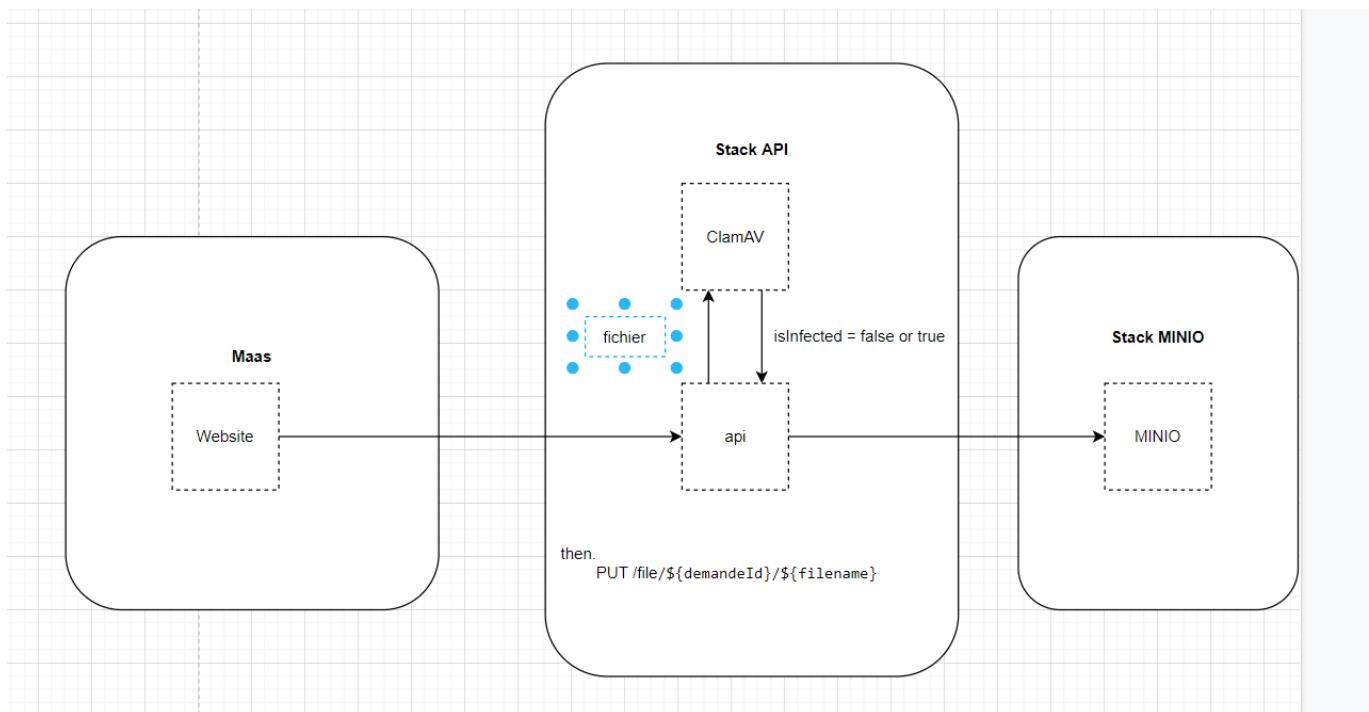


Figure 26 – Fonctionnement de l'Antivirus ClamAV

7.14. Tests d'intrusion / Revues de Code Source

Une campagne de tests d'intrusion a été menée par une équipe spécialisée en cybersécurité sur une instance de la plateforme. Les vulnérabilités remontées ont été traitées.

Une analyse statique de sécurité du code (SAST) est exécutée périodiquement sur le code source du produit. Les vulnérabilités détectées sont traitées au fur et à mesure.

7.15. Limitation volumétrique

7.15.1. Trafic entrant

Le contrôleur Ingress permet de mettre en œuvre du rate-limiting / throttling permettant de limiter le taux de sollicitation des APIs.

7.15.2. Taille max upload justificatif

Le filtrage de la taille maximum des pièces jointes et justificatifs uploadés est mis en œuvre. La taille maximale définie est 10 MB par fichier et est paramétrable.

7.16. Anti-DDoS

L'outil NGINX ModSecurity WAF est mis en œuvre pour protéger l'application contre les attaques DDoS en traitant les requêtes dans un seul thread de manière asynchrone, offrant ainsi une faible utilisation de la mémoire.

7.17. Cloisonnement

7.17.1. Cloisonnement zones

Le système est découpé en zone cloisonnées (zone front-end, zone applicative, zone données, zone administration fonctionnelle, zone logging, supervision & monitoring).

7.17.2. Cloisonnement réseau

Les réseaux sont cloisonnés en VPC, VLAN / subnet.

7.18. Système de détection d'intrusion

La détection d'intrusion est basée sur l'analyse des logs de journalisation.

7.19. Montée de version des systèmes d'exploitation et patchs sécurité

L'ensemble des actions de montée de version des systèmes d'exploitation et de mise à jour des patchs sécurité est réalisé par l'équipe d'exploitation.

8. Modèle de dimensionnement théorique

Le **dimensionnement théorique de l'environnement de production** du système est basé sur :

- les entrants fournis par le GART,
- les hypothèses proposées par Capgemini,
- les retours d'expérience de Capgemini dans le cadre de projets similaires,
- des métriques et des abaques.

L'ensemble de ces éléments a permis de réaliser un premier modèle de dimensionnement théorique du système moB.

8.1. Entrants du GART

ENTRANTS	PMV	Cible basse	Cible haute	Commentaires
Nombre utilisateurs (citoyens / usagers)	20 000	100 000	1 000 000	
dont chômeurs	1 620	8 100	81 000	8,10%
dont situation de handicap	74	370	3 700	0,37%
dont détenteurs du permis de conduire (B)	6 600	33 000	330 000	33%

8.2. Hypothèses de Capgemini

Hypothèses	PMV	Cible basse	Cible haute	Commentaires
Nombre MaaS (en moyenne)	1	3		PMV : 1 région, Cible : 3 régions
Nombre MSP (en moyenne)	5	15		

Hypothèses	Valeur	Unité	Commentaires
Pourcentage connexions concurrentes	20	%	
Durée session (en moyenne)	180	secondes	
Think-time	30	secondes	
Taille profile utilisateurs	5	Ko	
Nombre demandes subventions (en moyenne)	5	demandes par mois	
Taille justificatif (en moyenne)	200	Ko	
Nombre justificatifs (en moyenne) par demande	2		
Taille enreg demande	1	Ko	
Durée rétention	24	mois	

Nombre offres (en moyenne) par MSP	10	offres	
Taille offre (moyenne) pour MSP	1	Mo	
Taille offres (moyenne) MSP par MaaS	50	Mo	
Taille offre (moyenne) pour MaaS	10	Mo	
Taille offres (moyenne) MaaS	60	Mo	
Tracking GPS	N/A		

8.3. Modèle de dimensionnement théorique

Dimensionnement	PMV	Cible basse	Cible haute	Commentaires
Nombre connexions concurrentes	1 000	5 000	50 000	
Nombre calls APIs par seconde	33	167	1 667	
Nombre calls SQLs par seconde	167	833	8 333	
Taille offres (moyenne) (en Mo)	60	180		
Taille données utilisateurs (en Go)	920,20	4 601,00	46 010,02	Données utilisateurs : profile + demandes + justificatifs (24 mois)

9. Processus de livraison

9.1. Préparation et définition des jobs de livraison

9.1.1. Préparation de la branche réceptionniste Ops

En préparation du commit de livraison par l'équipe Dev dans le repo Git de l'équipe des opérations, les actions suivantes sont requises côté Ops :

- Coté Nexus :
 - Configuration d'un repo Docker dédié OPS, pour héberger les images : [docker-repo-ops](#) ;
 - Configuration d'un repo Helm, pour gérer les Helm charts : [Helm-charts](#);
- Coté Gitlab :
 - Sur le repo des OPS (**infrastructure**)
 - La création d'une branche réceptionniste : [delivery-ops](#) ;
 - La préparation des variables d'environnements CI/CD ;
 - La préparation des environnements KUBERNETES PREPROD et PROD(via les agents) ;
 - Protection des déploiements PREPROD et PROD par des approbations
 - *-preprod/*
 - *-prod/*

9.1.2. Définition de la pipeline de déploiement

Prérequis

GitLab Runners

Les stages de la pipeline ont besoin de runners qui doivent être bien configurés pour chaque environnement.

Les tags nécessaires pour chaque runner par environnement sont :

- Préproduction
 - os:linux, platform:**preprod**, task:configure, task:deploy, task:test
- Production
 - os:linux, platform:**production**, task:configure, task:deploy, task:test

Un runner par environnement a été mis en place.

Cluster Role binding

Le manifest du cluster role binding est le suivant, à créer sur le cluster via la ligne de commande :

```
apiVersion: rbac.authorization.k8s.io/v1
```

```

kind: ClusterRoleBinding
metadata:
  name: gitlab-group-cluster-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts

```

Storage classes

2 classes de stockage *kubernetes.io/azure-file* sont requises avec une policy par défaut à « Retain » pour les services suivants :

- bus
 - o volumeBinding : Immediate
- s3
 - o volumeBinding : WaitForFirstConsumer

Stages

Concernant la définition de la Pipeline du déploiement, les stages suivants ont été identifiés et sont à fournir côté équipe de développement :

- Stage 1 : Configure_preprod

Ce stage permet de générer les fichiers de configuration applicatifs (idp & bus) avec les valeurs de préproduction. Ce stage est optionnel et pourra être déclenché quand des modifications seront à apporter. Les fichiers sont générés dans un artefact pour faciliter leur récupération par l'équipe ops. Le déclenchement ainsi que la procédure sera spécifié pour les releases en ayant besoin. Les artefacts sont disponibles pendant 3js.

- Stage 2 : Deploy_preprod

Ce stage contiendra les jobs de déploiement des services de l'application. Le déploiement se fait sur le même namespace pour tous les services grâce à une variable CI/CD dans le repo cloud.

- Stage 3 : Test_preprod

Ce stage contiendra les jobs des tests automatisés à exécuter après le déploiement de la release en préproduction. Smoke-test pour vérifier que les services sont bien lancés. Un rapport html est généré en artefact qui sera disponible 3js.

- Stage 4 : Configure_production

Ce stage permet de générer les fichiers de configuration applicatifs (idp & bus) avec les valeurs de production. Ce stage est optionnel et pourra être déclenché quand des modifications seront à apporter. Les fichiers sont générés dans un artefact pour faciliter la

récupération par l'équipe ops. Le déclenchement ainsi que la procédure sera spécifié pour les releases en ayant besoin. Les artefacts sont disponibles pendant 3js.

- Stage 5 : Deploy_production

Ce stage contiendra les jobs de déploiement des services de l'application. Le déploiement se fait sur le même namespace pour tous les services grâce à une variable CI/CD dans le repo cloud.

- Stage 6 : Test_production :

Ce stage contiendra les jobs des tests automatisés à exécuter après le déploiement de la release en production. Smoke-test pour vérifier que les services sont bien lancés. Un rapport html est généré en artefact qui sera disponible 3js.

Considérations

Les jobs de ces stages seront déployés manuellement, une validation est requise de la part de l'équipe Ops via les approbations GitLab (Merge & Start Job).

Les jobs de déploiement ne contiennent pas le code source des applications, ils contiennent seulement les jobs permettant la configuration des environnements et le déploiement des charts Helm sur les clusters AKS.

Aucun déploiement de jobs *_prod_deploy et Test_prod en production sans passage/validation des jobs *_preprod_deploy et Test_preprod.

L'accès à ces éléments doit être restreint à l'équipe des opérations.

Actions communes figées par ordre pour l'ensemble des déploiements :

- Déploiement de la release ;
- Exécution des tests ;

Les autres actions spécifiques à la release seront mentionnées au niveau du mail officiel de la demande de la livraison avec des étapes de déroulement si ces étapes ne sont pas présentes sur ce document.

9.1.3. Schémas de déploiement DevOps

Côté Dev (testing + handover)

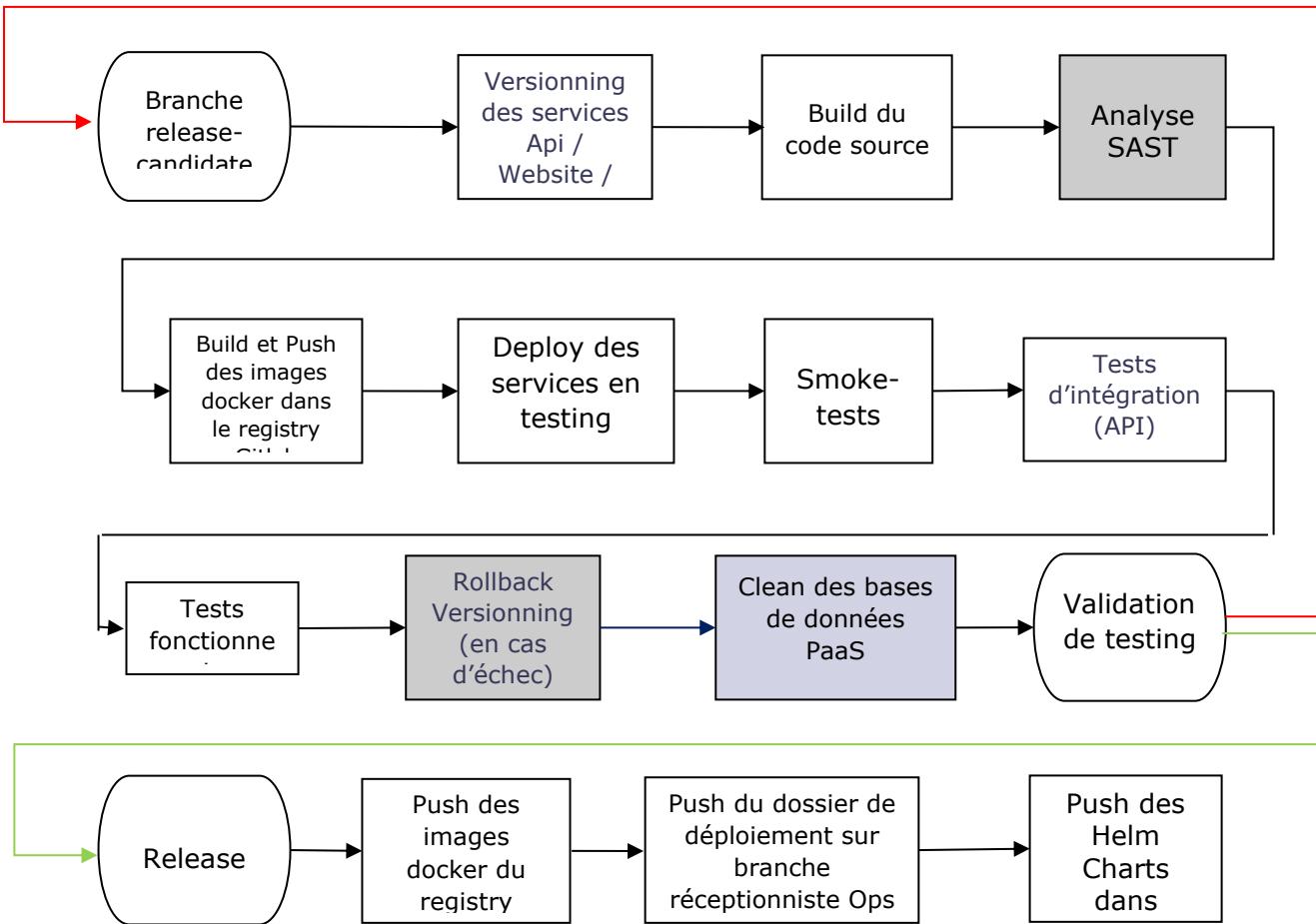
Action des développeurs

Stages de la pipeline

Stages optionnels

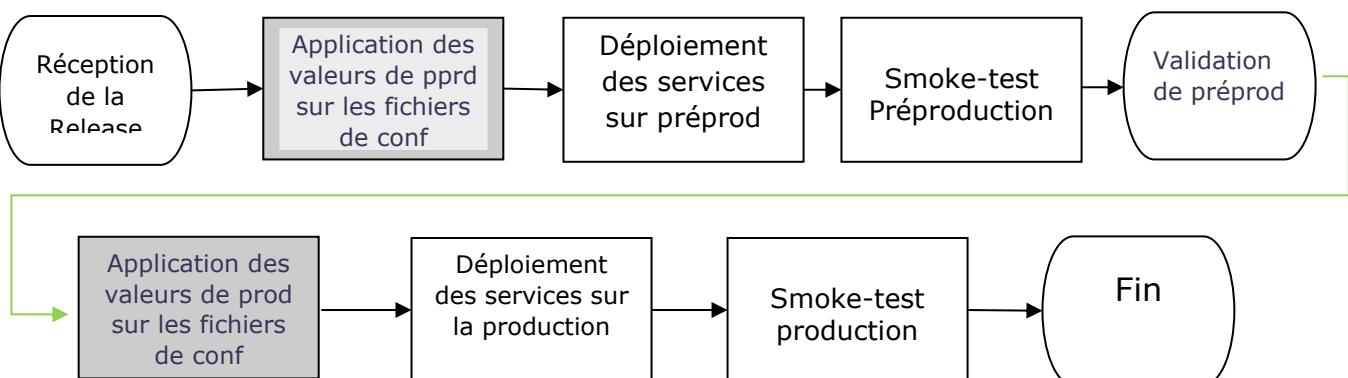
→ Validation

→ Invalidation



Côté Ops (préprod et prod)

- () Action des opérateurs
- () Stages de la pipeline
- (■) Stages optionnels
- Validation
- Invalidation



9.2. Livrables

L'équipe DEV délivre 3 types de contenus à l'équipe OPS.

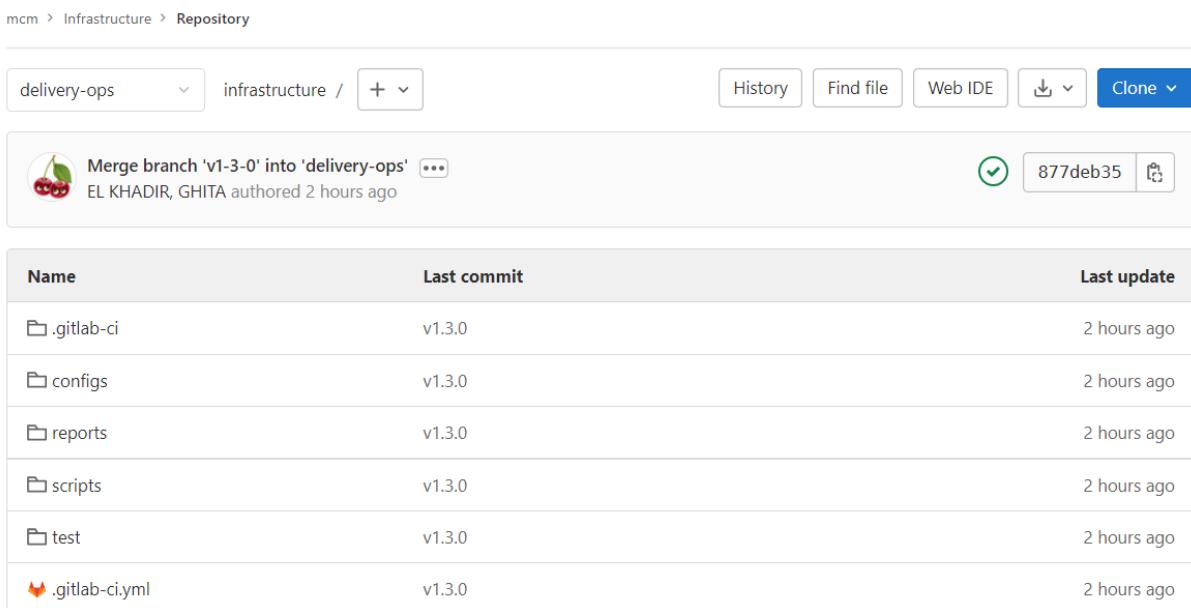
9.2.1. Images Docker

Les images standard et publiques se trouvent toujours dans le repository nexus docker-hub. Lorsqu'un service s'appuie sur une telle image, si l'image n'est pas présente dans le dépôt, elle sera téléchargée à partir du [Docker Hub](#) (pas d'authentification nécessaire) afin d'être mise en cache dans ce repository nexus.

Les images spécifiques, produites à partir du code source moB, sont présentes dans le repository nexus docker-repo-ops. On y trouve un seul dossier platform car les images ne diffèrent pas selon l'environnement sur lequel on déploie. Dans platform, les images se trouvent dans le dossier de la release à livrer.

9.2.2. Dossier de déploiement

Le dossier de déploiement livré aux Ops présente l'arborescence ci-dessous.

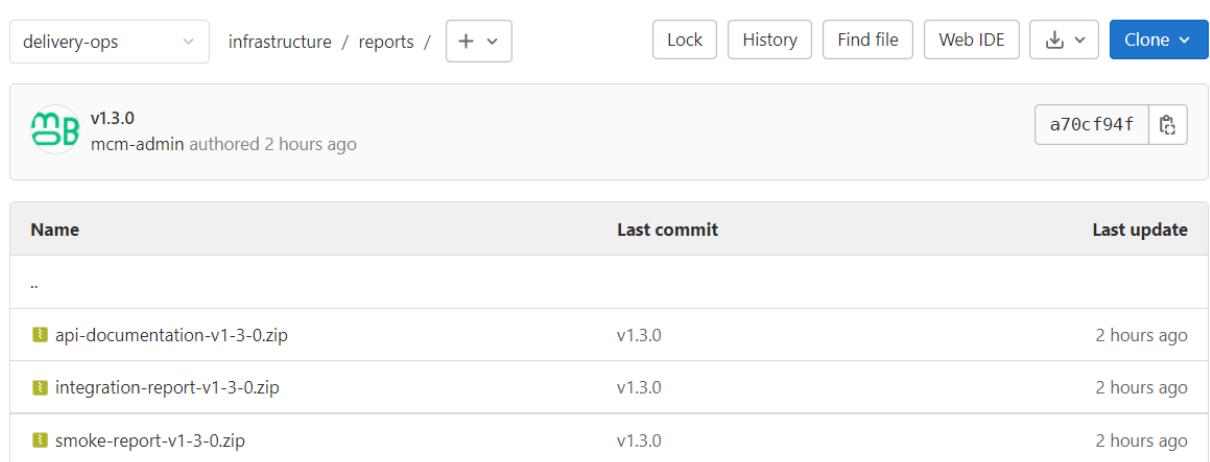


Name	Last commit	Last update
.gitlab-ci	v1.3.0	2 hours ago
configs	v1.3.0	2 hours ago
reports	v1.3.0	2 hours ago
scripts	v1.3.0	2 hours ago
test	v1.3.0	2 hours ago
.gitlab-ci.yml	v1.3.0	2 hours ago

L'équipe Dev transmet dans les dossiers suivants :

- /configs : les fichiers variabilisés de configuration idp et bus
- /reports
 - o Api-documentation : Extraction de l'openapi.json à visée des partenaires.
 - o Integration-report : Rapport des tests d'intégrations exécutés sur testing
 - o Smoke-report : Rapport des smoke tests exécutés sur testing
 - o Functional-report : Rapport des tests fonctionnels exécutés sur testing (non fonctionnel pour l'instant)

Ces rapports permettent de témoigner que les évolutions fonctionnelles et techniques apportées par la release ont bien été validées.



The screenshot shows a repository interface with the following details:

- Repository path: delivery-ops / infrastructure / reports
- Commit ID: v1.3.0
- Author: mcm-admin
- Date: authored 2 hours ago
- SHA: a70cf94f
- Clone button

Name	Last commit	Last update
..		
api-documentation-v1-3-0.zip	v1.3.0	2 hours ago
integration-report-v1-3-0.zip	v1.3.0	2 hours ago
smoke-report-v1-3-0.zip	v1.3.0	2 hours ago

- /scripts : les scripts de bases de données
- /test : permet de lancer les smoke tests via les pipelines
- ./gitlab-ci : les fichiers yml des pipelines pour pprd/prod

9.2.3. Helm Charts

Les packages helm sont disponibles dans le repository nexus Helm-charts. On trouve alors deux dossiers :

- platform-pprd
- platform-prod

Chacun de ces dossiers contiennent les packages pour la release. Seules les valeurs spécifiques à l'environnement diffèrent (helm values).

10. Approche DevOps

Le style d'architecture choisi — orienté microservices — conduit à un nombre important d'unités de déploiement. En outre, le passage à l'échelle implique une multiplication des instances/replicas. Par ailleurs, par rapport à une approche monolithique, le caractère distribué du système introduit de la complexité supplémentaire : les appels inter-services qui jusqu'ici étaient in-proc sont maintenant distants, visibles de l'extérieur. Ces appels sont par conséquent sensibles aux aléas du réseau et sont susceptibles d'échouer plus fréquemment.

Toutes ces raisons font qu'il est hautement désirable d'introduire certaines contre-mesures :

- Une stratégie de test appropriée devrait être mise en œuvre ; celle-ci requiert la capacité de créer de multiples environnements, à la demande ;
- Des patterns de stabilité tels que les timeouts, les circuit breakers, etc. devraient être implémentés ;
- Un monitoring de bout en bout devrait être implémenté afin d'identifier rapidement tous incident pendant l'exploitation ;
- L'environnement de production devrait utiliser les mêmes binaires que ceux de validation ; la structure de ces environnements devrait être identique ; la configuration devrait être réalisée au moyen de variables d'environnement ;
- Toutes les opérations de déploiement devraient être automatisées de façon à éviter les erreurs et pour pouvoir récupérer rapidement.

Des scripts sont communément utilisés pour automatiser les opérations de build, test et déploiement. Le principal inconvénient est qu'il s'agit d'une approche impérative qui impose à l'auteur des scripts de connaître l'état initial du système ainsi que toutes les opérations nécessaires pour atteindre l'état cible. Une attention particulière est alors requise pour s'assurer que ces scripts soient idempotents.

Dans le but de rendre le système le plus déterministe possible, nous préconisons d'éviter tout script impératif et de favoriser une approche déclarative. C'est la raison pour laquelle nous envisageons de recourir à Terraform et/ou Ansible pour toutes les tâches bas niveau de déploiement et sur des manifestes Kubernetes pour le déploiement d'applications, sachant que ces technologies encouragent nativement un style déclaratif.

Une dernière qualité opérationnelle souhaitable est la capacité de conserver un historique de tous les déploiements et d'avoir la possibilité de revenir à un état antérieur si nécessaire. Malheureusement, ceci n'est pas proposé par Kubernetes. Une fois qu'un manifeste est soumis, l'orchestrateur ne se souvient plus de l'état précédent du cluster. De plus, les déploiements ne sont pas transactionnels et peuvent laisser le système dans un état imprévisible en cas de problème.

10.1. Introduction à GitOps

Le problème exposé ci-dessus peut être résolu en adoptant une approche à 2 niveaux appelée « GitOps ». Ce concept peut être défini par la formule suivante :

*Tout en tant que code + Configuration déclarative + Gestion de versions +
Pull/Merge requests + Opérateur de réconciliation*

=

Déploiement automatique dans Kubernetes

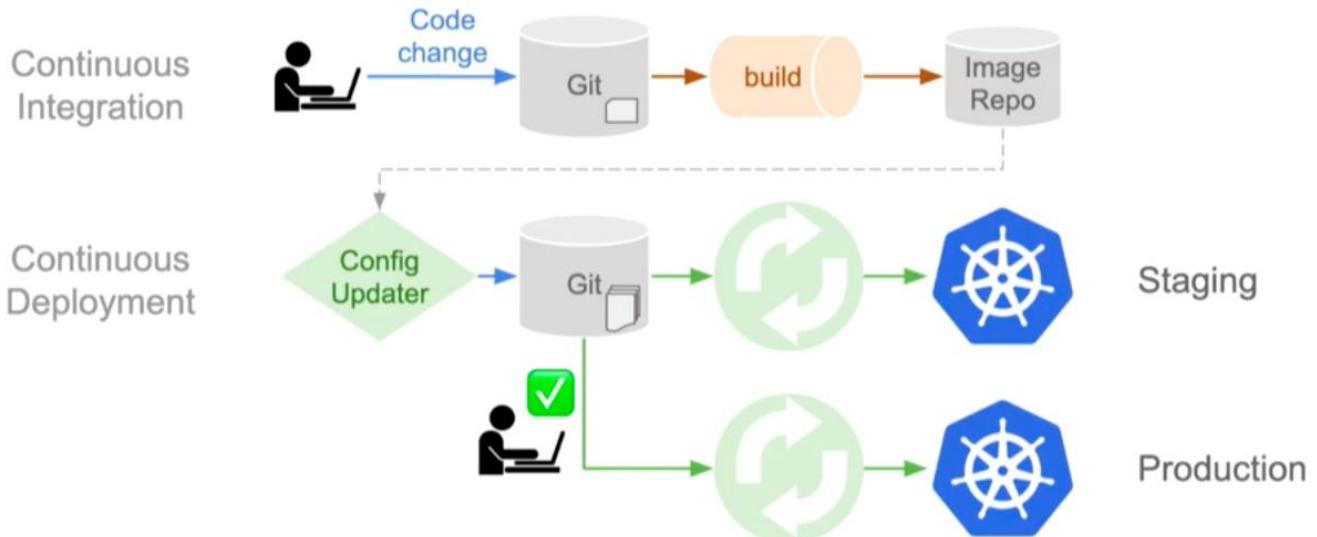


Figure 27 – Principes de GitOps

Source : <https://www.weave.works/blog/automate-kubernetes-with-gitops>

La première partie du flux de travail est une intégration continue classique : lorsque les développeurs soumettent des modifications de code dans le dépôt git, un pipeline de construction et d'intégration est automatiquement déclenché. Puisque nous construisons un système basé sur des microservices, le pipeline devrait produire des images de conteneurs stockées dans un référentiel d'images.

Le déploiement continu est géré par un outil spécial appelé Réconciliateur (Config Updater) : il est chargé de récupérer la dernière version des manifestes de déploiement, de les mettre à jour avec les versions d'image appropriées et de soumettre le résultat final dans un second dépôt git dédié aux opérations. Enfin, au lieu de pousser la configuration vers le paysage cible, un service dédié s'exécutant à l'intérieur du cluster Kubernetes est chargé d'extraire les manifestes de git et de les appliquer de manière transactionnelle.

10.2. Implémentation

Nous avons exposé au cours des paragraphes précédents l'approche que nous préconisons pour la chaîne de déploiement continu. Elle devrait présenter les caractéristiques suivantes :

- Recourir à l'Infrastructure as Code pour automatiser intégralement le déploiement de l'infrastructure aux couches applicatives.
- Faire de Git le point d'entrée unique pour la gestion de l'infrastructure et les déploiements applicatifs. Promouvoir les builds à l'aide des mécanismes de Pull/Merge Requests.
- Adopter un style purement déclaratif.
- Réserver un dépôt pour le code applicatif et un autre référentiel distinct pour l'infrastructure et la mise en production.
- Gérer l'état de Kubernetes à l'aide d'un opérateur déployé dans chaque cluster. L'opérateur surveille le dépôt Git approprié et répond aux événements pertinents (commits, pushes, tags).

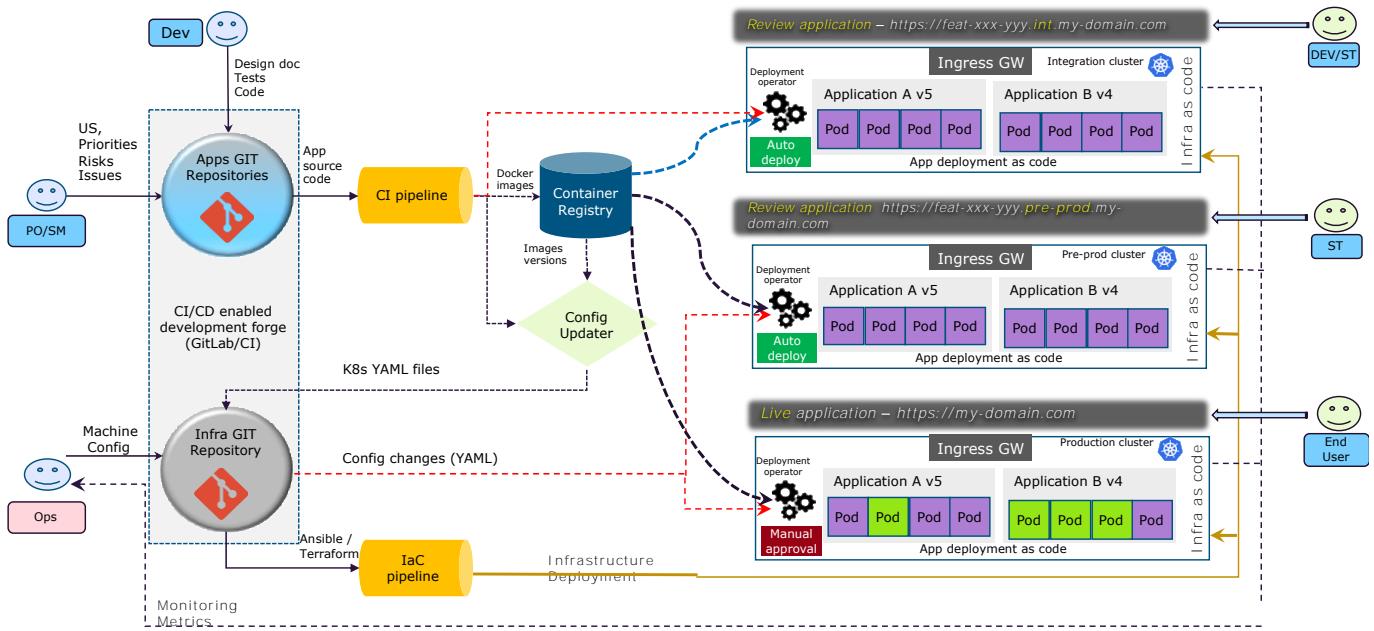


Figure 28 – Approche DevOps : orientation GitOps

Le réconciliateur est déclenché par l'équipe de développement lorsqu'elle considère le seuil de qualité atteint. Cela peut être fait à partir d'une exécution du pipeline de build existante et réussie en lançant manuellement une tâche supplémentaire dédiée. Le réconciliateur ne pousse que les manifestes compilés et la configuration vers le dépôt Git réservé à l'infrastructure. Cela déclenche un déploiement immédiat dans le cluster de préproduction sans rien reconstruire. L'opérateur du cluster de préproduction extrait simplement les bonnes images du registre de conteneurs et crée les services décrits dans les manifestes.

Enfin, une opération manuelle est nécessaire pour provoquer le déploiement final dans l'environnement réel de production.

Nous préconisons l'emploi de GitLab qui fournit en un seul outil une expérience intégrée couvrant l'ensemble du cycle de développement.

Par ailleurs, nous recommandons également de mettre en place :

- 1 dépôt unique avec une seule branche pour la gestion des infrastructures.
 - 1 dépôt unique pour l'ensemble du code applicatif. Organiser les modules dans une hiérarchie de dossier, selon une approche monorepo pour simplifier la gestion des dépendances.
- Le pipeline doit être conçu de sorte à construire et déployer uniquement les modules modifiés

10.3. Pipelines de build et déploiement

10.3.1. Inclusion dans le processus de livraison

Voir paragraphe « Processus de livraison ».

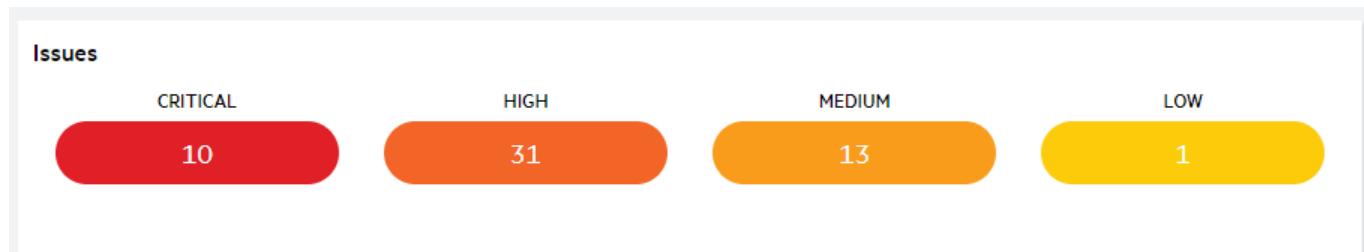
10.3.2. Procédure de publication du code

Une publication du code est effectuée périodiquement, plusieurs étapes ont été définies pour mener à bien cette procédure.

Analyse SAST

Mise en place d'une analyse SAST (Static Application Security Testing) du code permettant de détecter les anomalies critiques/majeurs potentielles à corriger avant la mise en production du PMV et la publication du code. L'analyse a été effectuée en utilisant l'outil « [Fortify On Demand](#) », paramétré pour analyser la branche principale du projet.

L'analyse permet de remonter les vulnérabilités potentielles classées en 4 criticités : critiques, hautes, moyennes et faibles, comme le montre un tableau résultat exemple ci-dessous :



Ces vulnérabilités sont traitées au fur et à mesure en amont de chaque publication. Certaines restent en l'état car non applicables dans le contexte d'utilisation du projet.

Nettoyage de code

Le nettoyage du code est essentiel avant la publication de celui-ci. Plusieurs actions ont été identifiées :

- Déterminer le périmètre et les parties de code à publier.
- Nettoyer le code d'éventuels mots de passe et liens référencés en dur dans le code en utilisant des variables
- Vérifier les noms des variables, des fonctions et commentaires à traduire en anglais
- Vérifier le contenu des TU et des mocks.

Documentation

La documentation est l'un des points nécessaires à mettre en place avant de prévoir une publication.

Les documents tel que ce DAT, les cas d'utilisation, le guide de configuration et d'exploitation sont essentiels. Un répertoire *docs* a été créé afin de référencier tous ces documents importants.

Pipeline de publication

Lorsqu'une branche est livrée aux OPS, un tag est posé. La pipeline de build peut permettre la publication de code sur un repository GitHub dont les informations sont paramétrées dans les variables de CI/CD de GitLab.

Afin de publier le code il est impératif de sélectionner un tag, et de passer en variable de lancement de la pipeline la variable PUBLISH_CODE avec comme valeur « true ».

Ainsi au lieu de lancer la pipeline de build c'est une pipeline de publication du code qui se déclenche. Une branche est créée sur le repository GitHub basé sur le nom du tag et une pull request est ouverte.

