Université Assane Seck de Ziguinchor

UFR Sciences et Technologies

Département Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de master

Mention : Informatique

Spécialité : Génie Logiciel

Sujet :

Système de contrôle d'accès pour les sociétés implantées au sein de la plateforme de distribution du Port Autonome de Dakar

Présenté et soutenu par :

M. Balla GNINGUE

le :

17 / 04 / 2024

Sous la direction de :

Dr Gorgoumack SAMBE

M. Moussa DIOP

Sous la supervision de :

Pr Khadim DRAME

Membres du jury :

Pr Ousmane DIALLO	Professeur assimilé	Président / Examinateur	UASZ
Pr Ibrahima DIOP	Professeur assimilé	Rapporteur	UASZ
Dr Gorgoumack SAMBE	Maitre de conférences titulaire	Encadrant	UASZ
Pr Khadim DRAME	Professeur assimilé	Co-Encadrant	UASZ
M. Moussa DIOP	Directeur Atlantic DS	Co-Encadrant	ADS

Année universitaire 2022-2023

Résumé

La plateforme de distribution constitue un réseau intégré d'infrastructures et de procédures instaurées dans le dessein de faciliter le mouvement efficient des marchandises et des cargaisons au sein du port de Dakar, situé au Sénégal.

Actuellement, le contrôle d'accès au niveau de la plateforme de distribution est géré manuellement. Cependant, ce mode de gestion présente des vulnérabilités, notamment des risques d'accès non autorisés et des complexités sur la gestion des mouvements d'entrée et de sortie des individus et des véhicules. Ces défis suscitent des préoccupations quant à la sécurité des marchandises et des installations portuaires.

Afin de résoudre ces problématiques, nous avons réalisé un système sécurisé, centralisé et basé sur des rôles, répondant aux objectifs majeurs suivants : la gestion des accès et des sociétés locataires, la gestion des ressources (personnel et véhicules), la gestion des espaces de stationnement, la définition de profils d'accès personnalisés, l'attribution de badges et le suivi des entrées/sorties.

De manière spécifique, notre solution comprend la mise en place d'une API indépendante permettant aux sociétés d'intégrer notre système à leurs applications, ainsi que des interfaces conviviales pour une utilisation facile par les utilisateurs.

Dans cette démarche, nous avons choisi d'adopter la méthodologie Scrum pour la gestion de projet, d'établir une architecture en microservices. De plus, le système de contrôle d'accès s'appuie sur la technologie RFID. Pour démontrer son fonctionnement, nous avons élaboré un prototype physique à l'aide de montages arduino mais aussi une simulation virtuelle sur ordinateur.

L'initiative présente une première version du système de contrôle d'accès, visant à résoudre des problèmes cruciaux de sécurité et d'efficacité. Ces avancées jettent les bases d'une solution complète, parfaitement alignée sur les exigences strictes du commerce international.

Mots clés : Plateforme de distribution, contrôle d'accès, Port autonome de Dakar, RFID

Abstract

The distribution platform constitutes an integrated network of infrastructures and procedures established with the purpose of facilitating the efficient movement of goods and cargo within the Port of Dakar, located in Senegal.

Currently, access control at the distribution platform is managed manually. However, this mode of management presents vulnerabilities, including risks of unauthorized access and complexities in managing the entry and exit movements of individuals and vehicles. These challenges raise concerns about the security of goods and port facilities.

To address these issues, we have developed a secure, centralized, and role-based system that meets the following major objectives: access management for tenant companies, resource management (personnel and vehicles), parking space management, customized access profile definition, badge assignment, and precise tracking of entries and exits.

Specifically, our solution includes the implementation of an independent API that allows companies to integrate our system with their existing or future applications, as well as user-friendly interfaces for easy and intuitive system use.

In this endeavor, we have chosen to adopt the Scrum methodology for project management and to establish a microservices architecture. Furthermore, the access control system relies on RFID technology. To demonstrate its operation, we have developed a physical prototype using Arduino setups, as well as a virtual computer simulation.

This initiative presents the first version of the access control system, aiming to address crucial security and efficiency issues. These advancements lay the foundation for a comprehensive solution, perfectly aligned with the stringent requirements of international trade.

Keywords: Distribution platform, access control, Autonomous Port of Dakar, RFID

Remerciements

En cette étape cruciale de mon parcours académique et professionnel, je tiens à exprimer ma gratitude envers le Tout-Puissant, source de toute grâce et de toute opportunité, ainsi qu'à mes chers parents et à ma famille pour leur soutien inconditionnel et leurs sacrifices qui ont tracé le chemin de cette réussite.

Je remercie sincèrement M. Moussa DIOP pour sa guidance éclairée, sa bienveillance et sa disponibilité pendant mon stage. Son soutien et l'opportunité qu'il m'a offerte d'évoluer au sein de son entreprise ont enrichi mon expérience et renforcé mes compétences.

Mes remerciements vont également à mes encadrants de mémoire, le Pr Khadim DRAME et le Dr Gorgoumack SAMBE, pour leur humilité, leur engagement et leur précieux encadrement. Leur acceptation de m'encadrer, ainsi que leurs conseils avisés et leur soutien constant, ont été essentiels pour la qualité de mon travail.

Je souhaite exprimer ma profonde reconnaissance envers Pr Ousmane DIALLO pour avoir accepté de présider ce jury et Pr Ibrahima DIOP pour avoir accepté d'évaluer ce modeste travail.

Un immense merci également à mes tuteurs et familles d'accueil à l'université, Moustapha Ndiaye, Boubacar Senghor, Ibrahima Sène et Ababakr Sidki Dicko, pour leur accueil et leur hébergement.

Je tiens à exprimer ma gratitude envers le personnel de Business Logistique, IZICARS et particulièrement à l'équipe d'Atlantic Digital Solutions, spécialement à Mme SARR Rokhaya DIOP et à M. Pape Matar DIENG, pour leur accueil chaleureux, leur esprit d'équipe et leur accompagnement tout au long du stage.

Un merci particulier à Mouhamadou DIAMANKA pour sa précieuse collaboration.

Je suis profondément reconnaissant envers Oumar Ngala DIOUF (Timack), Astou Ndiaye Sarr, Waly Fall (Mame), Lamine Diaw et Maty Thiam (Frère) pour avoir consacré leur temps à la lecture de mon mémoire et à l'amélioration de son contenu.

Enfin, je souhaite exprimer toute ma gratitude à Omar SANE, Issakha FALL et Ellimane Fall pour leur encadrement et leur guidance tout au long de mon cursus.

Ces remerciements sont une humble expression de ma gratitude envers tous ceux qui ont rendu cette étape significative et m'ont permis de grandir professionnellement et humainement.

Dédicaces

À mes chers parents,

qui ne sont plus parmi nous mais dont la présence et le soutien continuent à m'inspirer chaque jour.

Vous m'avez inculqué les valeurs de persévérance, de travail acharné et d'intégrité qui m'ont permis d'atteindre ce moment important de ma vie

Que cette dédicace soit un humble hommage à votre vie et à votre amour qui resteront gravés dans mon cœur pour l'éternité,

***À mes sœurs**,*

vos encouragements constants et votre foi en mes capacités m'ont donné la détermination nécessaire pour poursuivre mes études avec passion et détermination.

À mes frères,

mes premiers modèles, mes premiers amis. Votre soutien inconditionnel et vos conseils avisés ont été mes guides tout au long de cette aventure académique,

À Ndeye Khady GNINGUE (Toucouleur),

pour sa présence constante à mes côtés, me rappelant que je ne suis jamais seul dans cette aventure,

À mes amis de toujours, Mussa, Chérif, Nash, Ngoné

pour leur présence rassurante et leur soutien infaillible,

À mes anciens camarades de chambre, Thierno Amar, Ndomi, Palaye, avec qui j'ai partagé tant de moments mémorable ,

À mes amis du primaire, collège, du lycée, de la S20, de la 4ème Promo MPI, du master GL & RS, de L'AERKM, du club Temple du Savoir, du Dahira DMNTKM,

À tous ceux qui ont croisé ma route et ont contribué, à leur manière, à la réussite de ce parcours académique, je vous adresse ma plus sincère gratitude. Ce mémoire est le fruit non seulement de mon travail, mais aussi de votre soutien et de votre inspiration. Merci du fond du cœur.

Tables des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ANPR	:	Automatic Number Plate Recognition
API	:	Application Programming Interface
CSS	:	Cascading Style Sheets
GIE	:	Groupement d'Intérêt Économique
HTML	:	Hypertext Markup Language
HTTP	:	Hypertext Transfer Protocol
IA	:	Intelligence Artificial
IDE	:	Integrated Development Environment
LCD	:	Liquid Crystal Display
PAD	:	Port Autonome de Dakar
REST	:	Representational State Transfer
RFID	:	Radio-Frequency Identification
SOA	:	Service Oriented Architectures
SOAP	:	Simple Object Access Protocol
TS	:	TypeScript
UML	:	Unified Modeling Language

Introduction générale

Au cœur des échanges internationaux, les ports occupent une position stratégique dans l'économie mondiale en facilitant le déplacement à grande échelle des marchandises. La gestion sécurisée et efficace des flux logistiques au sein des installations portuaires revêt une importance cruciale pour garantir l'efficacité des opérations et maintenir un niveau optimal de services.

C'est dans ce contexte que s'inscrit le thème de notre stage portant sur la mise en place d'un système de contrôle d'accès pour la plateforme de distribution du port autonome de Dakar, visant à sécuriser les accès pour préserver l'intégrité des marchandises et des installations portuaires.

Ce système est articulé en deux parties distinctes : la première concerne le contrôle d'accès pour le personnel et les véhicules des sociétés internes de la plateforme de distribution, tandis que la seconde s'adresse aux véhicules et au personnel des sociétés externes en relation avec les sociétés internes.

Dans ce projet, ma mission a consisté à approfondir la première partie, mettant en lumière les solutions et les processus spécifiques dédiés au contrôle d'accès pour le personnel et les véhicules des sociétés locataires.

La structure du mémoire explore différentes facettes du projet.

Le premier chapitre décrit la structure d'accueil du stage, ainsi que la présentation détaillée du sujet. Il englobe l'étude de l'existant, la problématique identifiée, ainsi que les objectifs du projet.

Le deuxième chapitre s'articule sur le cadre méthodologique et de développement qui a guidé notre démarche. Nous y exposons des méthodologies de gestion de projet, des architectures utilisées dans le monde du développement logiciel. Les choix stratégiques et technologiques retenus pour le développement du système de contrôle d'accès y sont également discutés.

Le troisième chapitre élargit notre compréhension des systèmes de contrôle d'accès physique en abordant leurs généralités. Une revue de la littérature y est menée, mettant en lumière les meilleures pratiques et les technologies émergentes telles que la RFID, la reconnaissance faciale, et les équipements de contrôle d'accès. Les choix spécifiques des technologies adoptées dans notre contexte y sont également exposés.

Dans le quatrième chapitre, nous analysons et spécifions les besoins spécifiques du Port Autonome de Dakar en matière de contrôle d'accès. Nous y approfondissons notre compréhension des exigences spécifiques afin de les traduire en critères fonctionnels et techniques.

Le cinquième chapitre approfondit la phase de conception du système, où nous explorons la définition de l'architecture générale. Ce volet englobe la structuration des microservices, l'élaboration de diagrammes de composants, de déploiement, de paquetage, ainsi que la conception des classes.

Le sixième chapitre se concentre sur l'implémentation pratique du système de contrôle d'accès et de la présentation des résultats obtenus.

Enfin, nous finirons par une synthèse et une proposition de perspectives d'évolution du système de contrôle d'accès toujours visant à satisfaire les exigences de la plateforme de distribution du port autonome de Dakar.

Chapitre 1 : Description du Sujet

Introduction

Dans l'ère de la révolution numérique, Atlantic Digital Solutions se positionne comme un intervenant spécialisé dans la digitalisation, proposant des services innovants. L'objectif de cette présentation est de souligner la contribution d'Atlantic Digital Solutions dans le domaine de la transformation digitale, affirmant son rôle en tant que partenaire stratégique pour les entreprises cherchant à s'adapter au paysage numérique en perpétuelle évolution. Dans cette optique, ce chapitre aspire aussi à fournir une vision complète du sujet en mettant en avant la présentation de la plateforme de distribution, les objectifs fixés, l'analyse de la situation actuelle, et en identifiant la problématique qui motive la conception d'un système de système de contrôle d'accès physique pour les piétons et les véhicules.

I. Présentation de la structure d'accueil

1. Mission

Chez Atlantic Digital Solutions, leur mission se concrétise par leur engagement à être le partenaire privilégié des entreprises embrassant leur transformation digitale. Ils consacrent à fournir à leurs clients une expertise et un savoir-faire pour la conception de produits uniques et sur mesure. Ces solutions sont élaborées en intégrant les dernières avancées technologiques, garantissant ainsi une approche innovante parfaitement adaptée au contexte spécifique de chaque entreprise.

2. Organisation

La **figure 1** montre l'organigramme de la structure de l'entreprise Atlantic Digital Solutions.

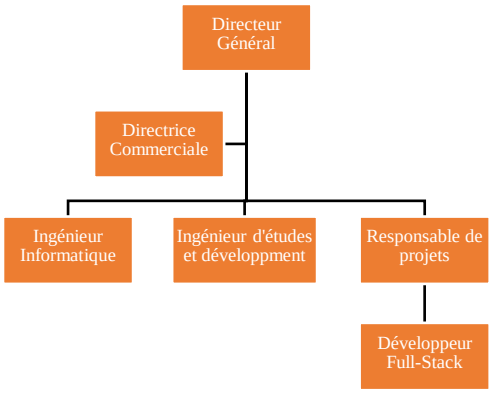


Figure 1 : Organigramme d'Atlantic Digital Solutions

3. Services

Atlantic Digital Solutions offre une gamme complète de services couvrant l'intégralité du spectre de la digitalisation. Du premier stade de la consultation en transformation digitale à la mise en œuvre pratique, notre entreprise propose des solutions holistiques. Cela englobe des consultations personnalisées, le développement sur mesure d'applications, l'intégration de systèmes et une gestion efficace des données. Chaque service est spécifiquement conçu pour répondre aux besoins uniques de chaque client, assurant une transition numérique réussie et adaptée à l'écosystème particulier de chaque entreprise. Nos services comprennent le développement d'applications mobiles, la création de logiciels sur mesure, l'hébergement et les noms de domaine, l'implémentation de modules ERP, la fourniture de licences Office et Kaspersky, ainsi que la gestion de parc informatique.

II. Contexte de stage

1. Présentation de la plateforme de distribution

La plateforme de distribution est un ensemble d'infrastructures, de services et de processus mis en place pour faciliter le flux efficace des marchandises et des cargaisons à travers le port de Dakar, au Sénégal. Elle vise à optimiser les opérations logistiques, à améliorer la productivité et à favoriser le commerce international.

Dotée d'une importante capacité de stockage, la plateforme de distribution abrite les infrastructures suivantes :

- 2 accès distincts ;
- 8 hangars ;
- 2 postes de gendarmeries ;
- 1 poste de douane ;
- 1 zone de dépotage ;
- 2 operateurs (TOM, CMA CGM) ;
- 1 parking véhicule ;
- 2 ponts bascules ;
- 1 pompe à essence.

La plateforme de distribution est concédée à un concessionnaire qui loue les espaces aux différents sociétés, et assure la gestion globale de la plateforme. Chacune des sociétés

implantées dans la plateforme s'occupe de son espace, et gère son flux de marchandises et de véhicules entrant et sortant.

La **figure 2** montre une vision satellitaire de la plateforme de distribution du port autonome de Dakar.

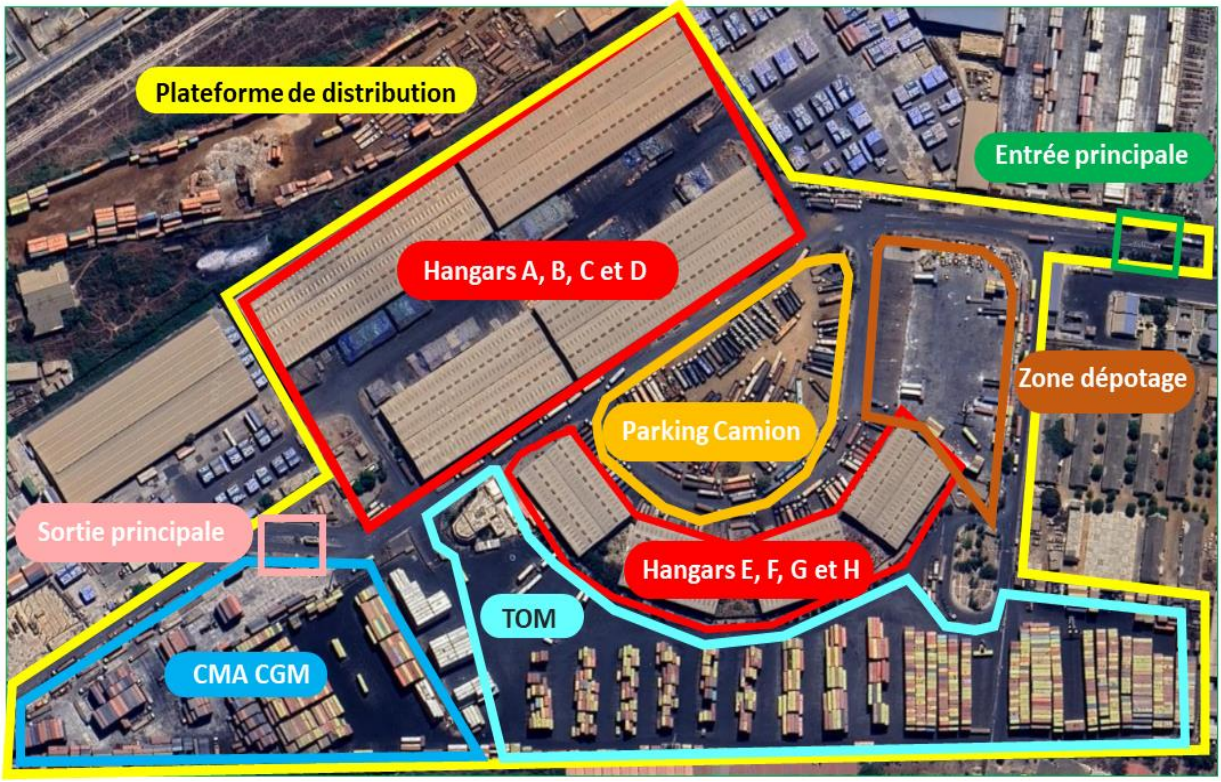


Figure 2 : Plateforme de distribution du port autonome de Dakar

2. Etude de l'existant

La Plateforme de distribution du port autonome de Dakar occupe une position centrale dans la coordination des opérations logistiques et de distribution. Deux accès distincts sont aménagés, chacun doté d'un poste de contrôle occupé par des agents, tels que ceux de la gendarmerie et des agents de sécurité de proximité.

L'analyse de la situation actuelle met en évidence divers aspects de cette plateforme, notamment la gestion des accès, l'attribution de badges, les sociétés établies, les relations avec les Groupements d'Intérêt Économique (GIE) et les opérations de distribution.

❖ **Gestion des accès et attribution de badges**

- Contrôle d'accès manuel : Actuellement, le contrôle d'accès à la plateforme de distribution est géré de manière manuelle à l'entrée et à la sortie, avec la présence constante de vigiles supervisant ces processus. Bien que la plateforme soit équipée de tourniquets, ceux-ci demeurent inutilisés par les piétons. Les véhicules doivent

franchir une barrière levante manuelle pour entrer et sortir, un processus géré par les vigiles.

- Badges Temporaires : la société concessionnaire de la plateforme de distribution fournit des badges temporaires aux sociétés établies, qui les attribuent à leurs visiteurs pour un accès temporaire à la plateforme.

❖ **Sociétés Implantées**

À l'intérieur de la plateforme, plusieurs sociétés ont établi leurs opérations, chacune disposant de ses propres employés, flotte de véhicules et besoins logistiques spécifiques. Ces sociétés opèrent de manière autonome pour gérer leurs opérations internes. De plus, elles entretiennent des relations commerciales avec des sociétés externes. Ces interactions comprennent la réception de marchandises provenant de fournisseurs externes ainsi que l'expédition de produits vers des clients externes. Les sociétés implantées agissent comme des nœuds essentiels dans la chaîne logistique de la plateforme, facilitant les échanges commerciaux entre différents acteurs du marché.

❖ **Relations avec les GIE**

Les sociétés établies collaborent étroitement avec des Groupements d'Intérêt Économique (GIE) pour l'approvisionnement en manœuvres nécessaires à leurs opérations logistiques. Les responsables de chaque GIE soumettent des demandes de badges d'accès pour leurs manœuvres auprès de la société concessionnaire de la plateforme de distribution. Ces badges sont valides pour une période définie, autorisant ainsi l'accès à la plateforme pour les manœuvres.

❖ **Opérations de distribution et de réception des marchandises avec les sociétés tierces**

Les sociétés externes sont les sociétés qui sont à l'extérieur de la plateforme et traitent avec les sociétés implantés pour des opérations de distribution et de réception de marchandises. Ces sociétés ont leur personnel et leurs propres camions qui, pour effectuer une opération au sein de la plateforme doivent avoir en possession un bon d'entrée délivré par la société destinataire.

Les opérations de distribution et de réception des marchandises constituent le pilier central des activités de la plateforme. Plusieurs mesures cruciales sont mises en place pour assurer leur bon déroulement :

- Contrôle d'accès des camions externes : Les camions des entreprises tierces doivent fournir un bon d'entrée à l'entrée de la plateforme, lequel est vérifié par le personnel de sécurité afin d'autoriser l'accès.
- Contrôle de sortie : Lorsque les camions quittent la plateforme, un bon de sortie est nécessaire. Ce document est soumis à une vérification et une validation par les autorités douanières, aussi bien pour les camions des entreprises externes que pour ceux des entreprises déjà établies sur le site.

Cependant, il est important de noter qu'en raison du manque d'espaces de stationnement à l'extérieur de la plateforme, certains véhicules ont été autorisés à entrer même sans raisons valables. Cette situation compromet la sécurité et l'efficacité du contrôle d'accès.

Bien que la présence des vigiles vise à renforcer la sécurité en surveillant attentivement les entrées et les sorties, en vérifiant les autorisations et en intervenant au besoin, elle ne résout pas entièrement le problème des accès non autorisés.

La **figure 3** suivante montre une illustration de l'existant

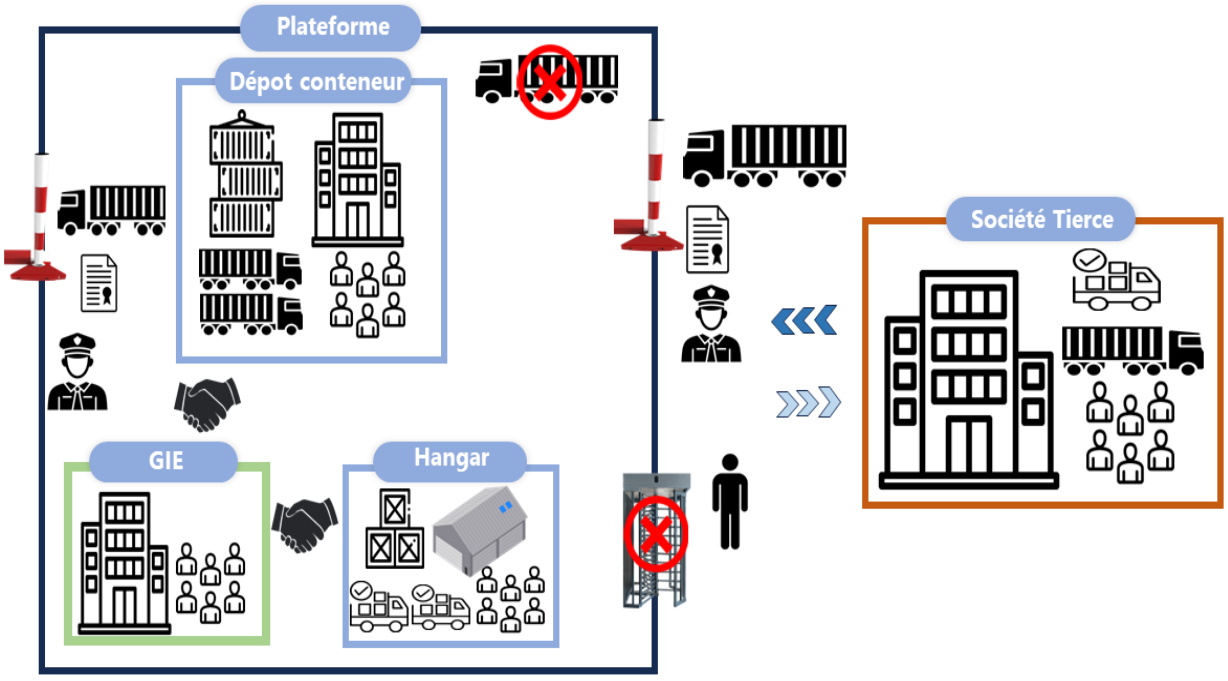


Figure 3 : illustration de l'existant

3. Limites de l'existant

Le système de contrôle d'accès actuel présente diverses limitations en matière de sécurité, de traçabilité et de gestion des autorisations, notamment :

- **Contrôle des intrusions** : Des accès non contrôlés peuvent être exploités par des individus non autorisés, accroissant les risques de vol, de sabotage, d'intrusion et d'activités criminelles. La nécessité de surveiller le stationnement des véhicules à l'intérieur de la plateforme de distribution est cruciale pour maintenir l'ordre et garantir la présence uniquement des véhicules autorisés, appartenant aux opérateurs, aux clients et aux visiteurs.
- **Inefficacité opérationnelle** : La gestion manuelle des entrées de véhicules ou de personnes par des vigiles présente des inconvénients tels que la lenteur du processus et le risque d'erreurs. Les vigiles peuvent également autoriser le stationnement de véhicules à l'intérieur de la plateforme par manque d'espace à l'extérieur, même s'ils ne sont pas autorisés.
- **Protection des marchandises** : La gestion manuelle du contrôle d'accès peut entraîner des risques de vol ou de détournement des marchandises stockées dans la plateforme, avec la possibilité d'accès non autorisés aux zones de chargement et de déchargement.
- **Gestion du flux de véhicules** : Un système de contrôle d'accès manuel complique la gestion efficace du flux de véhicules entrant et sortant de la plateforme, entraînant des retards dans les opérations de chargement et de déchargement.
- **Sécurité du personnel** : Un contrôle d'accès inadéquat peut compromettre la sécurité du personnel travaillant dans la plateforme, soulignant l'importance de limiter l'accès aux seules personnes autorisées et formées aux zones de travail.
- **Gestion des situations d'urgence** : En cas d'urgence, un système de contrôle d'accès devient essentiel pour gérer la situation en contrôlant le flux de personnes et de véhicules, facilitant ainsi l'évacuation ou l'intervention rapide des équipes de secours.

4. Objectif principal

L'objectif principal de notre mémoire consiste à mettre en œuvre un système de contrôle d'accès physique des piétons et des véhicules destiné aux personnels et aux véhicules entrant et sortant dans la plateforme de distribution du port autonome de Dakar. Ce système de contrôle d'accès comprendra non seulement les entrées et sorties principales, mais également chaque zone réservée à une société.

De manière spécifique, notre objectif principal comprend la mise en place d'une API sécurisée, indépendante et basée sur des rôles, permettant aux sociétés locataires d'intégrer notre système à leurs applications existantes ou futures. Nous proposons également des interfaces conviviales pour une utilisation facile et intuitive du système par les utilisateurs. Ces éléments visent à offrir

une solution technologique intégrée, alignée sur les besoins opérationnels spécifiques de la plateforme de distribution du port autonome de Dakar.

a. Délimitation du sujet

Ce projet de système de contrôle d'accès pour la plateforme de distribution du port autonome de Dakar est articulé autour de deux sous-projets distincts, chacun visant à répondre à des besoins spécifiques en matière de gestion des accès et de sécurité. Cette segmentation permet de concentrer les efforts sur des aspects particuliers du contrôle d'accès, tout en garantissant une approche adaptée aux différentes catégories d'utilisateurs de la plateforme.

- Sous-Projet 1 : Ce premier volet du projet est axé sur la mise en place d'un système de contrôle d'accès dédié aux personnels et aux véhicules des sociétés établies à l'intérieur de la plateforme de distribution.
- Sous-Projet 2 : Le deuxième volet du projet se concentre sur le contrôle d'accès des personnels et des véhicules des sociétés externes collaborant avec les sociétés implantées à l'intérieur de la plateforme de distribution.

Ces deux sous-projets complémentaires s'inscrivent dans une démarche globale visant à optimiser la gestion des accès et à renforcer la sécurité au sein de la plateforme de distribution du port autonome de Dakar.

Il est à noter que ce projet est mené en collaboration entre deux contributeurs (Mouhamadou DIAMANKA et Balla GNINGUE). Il existe à la fois des parties communes et des aspects spécifiques à chaque sujet. Chacun de nous, est chargé de son propre sous-projet : le sous-projet 1 pour ma part et le sous-projet 2 pour Mouhamadou DIAMANKA.

Cette approche assure une spécialisation et une expertise dédiée à chaque aspect du système de contrôle d'accès que nous développons conjointement

b. Objectifs spécifiques

Les objectifs spécifiques de notre solution informatique pour le contrôle d'accès à la plateforme de distribution du port autonome de Dakar incluent les aspects suivants :

- Centralisation de la gestion des sociétés locataires et de leurs ressources (personnel et véhicules) ;
- Gestion des espaces de stationnement des camions au sein de la plateforme ;
- Définition de zones et profils d'accès ;

- Attribution et révocation de badges ;
- Contrôle et supervision des entrées et sorties au sein de la plateforme ;
- Notifications en temps réel des accès et tentatives d'intrusion aux parties concernées ;
- Statistiques des entrées, des sorties, des disponibilités de place ;
- Visualisation des autorisations sur des accès de la plateforme.

Ces objectifs spécifiques orientent le processus de conception et de prototypage du système de contrôle d'accès, garantissant ainsi une solution adaptée aux exigences opérationnelles de la plateforme de distribution du port autonome de Dakar.

Conclusion

Dans ce premier chapitre dédié au cadre de stage et à la description du sujet, il ressort la contribution d'Atlantic Digital Solutions dans le domaine de la transformation digitale notre structure d'accueil et une vision approfondie de la plateforme du port autonome de Dakar. La présentation détaillée de ses dimensions, capacités, infrastructures, et flux logistiques offre une toile de fond essentielle pour comprendre les défis et les opportunités qui motivent ce projet d'optimisation des opérations de distribution. Les éléments ainsi présentés guideront le prototypage du système de contrôle d'accès dans les prochains chapitres.

Chapitre 2 : Cadre méthodologique et de développement

Introduction

Ce chapitre consacré au cadre méthodologique et de développement constitue un élément essentiel de ce projet, visant à explorer les fondements méthodologiques et techniques qui guideront le processus de développement du projet. L'adoption d'une bonne approche offre une structure dynamique et itérative, favorisant la flexibilité et la collaboration au sein de l'équipe de développement. En parallèle, l'utilisation d'une architecture de pointe se profile comme une réponse aux défis modernes de la complexité logicielle, en permettant une conception modulaire et évolutive. Cette section sert ainsi de toile de fond pour comprendre comment ces deux dimensions sont intégrées pour favoriser l'efficacité et la réussite du projet.

I. Cadre Méthodologique

La gestion de projet est définie comme l'application de connaissances, de compétences, d'outils et de techniques aux activités d'un projet dans le but de répondre à ses exigences. Afin de faciliter cette gestion, diverses méthodologies de gestion de projet ont été élaborées.

1. Les méthodes classiques

Les méthodologies de développement classiques se caractérisent par une approche séquentielle et linéaire du développement logiciel. Chaque phase, de la spécification à la maintenance, est réalisée de manière séparée, impliquant souvent une avancée étape par étape **[1]**.

Nous avons plusieurs méthodes traditionnelles à disposition, mais nous nous concentrerons principalement sur le développement en cascade et en V.

- **Modèle en Cascade (Waterfall)**

Cette méthode repose sur la succession d'étapes prédéfinies, sans la possibilité de revenir en arrière. Chaque phase doit être complétée avant de passer à la suivante, ce qui signifie que le processus avance de manière séquentielle, en cascade, d'où le nom **[1].**

Bien que la méthode en cascade soit simple à comprendre et à mettre en œuvre, elle présente certains inconvénients. Par exemple, les changements de besoins en cours de route peuvent être

difficiles à intégrer car chaque phase dépend des livrables de la phase précédente. De plus, le client peut ne pas voir de résultats tangibles avant la fin du processus, ce qui peut être frustrant.

La **figure 4** montre la succession des étapes du modèle en cascade.

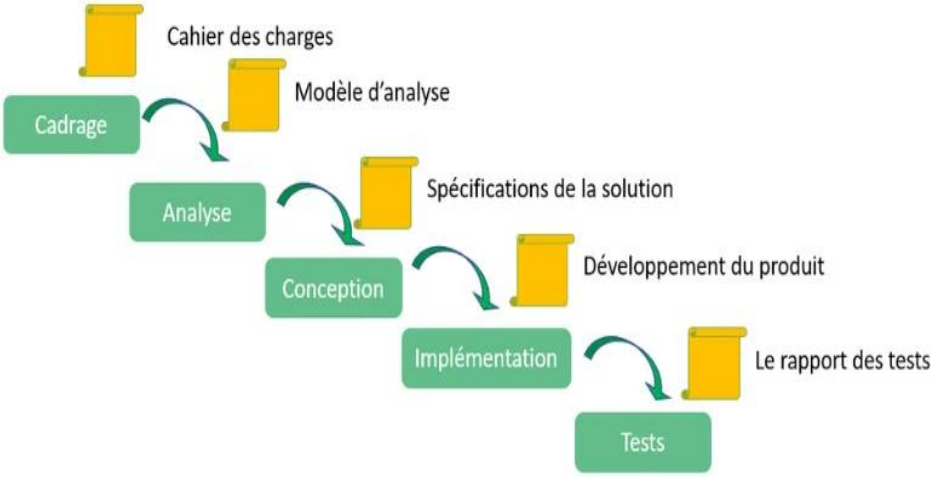


Figure 4 : Méthode en cascade

❖ **Modèle en V**

C'est une méthode de gestion de projet réputé pour son organisation des activités en deux flux parallèles. Elle peut être considérée comme un prolongement et amélioration du modèle en waterfall **[2]**.

Ce modèle met davantage l'accent sur la validation et la vérification à chaque étape du processus de développement, ce qui aide à réduire les risques liés aux défauts logiciels. Cependant, il reste une approche linéaire et séquentielle, ce qui peut rendre difficile l'adaptation aux changements de besoins en cours de route.

La **figure 5** montre les principales étapes du modèle en V.

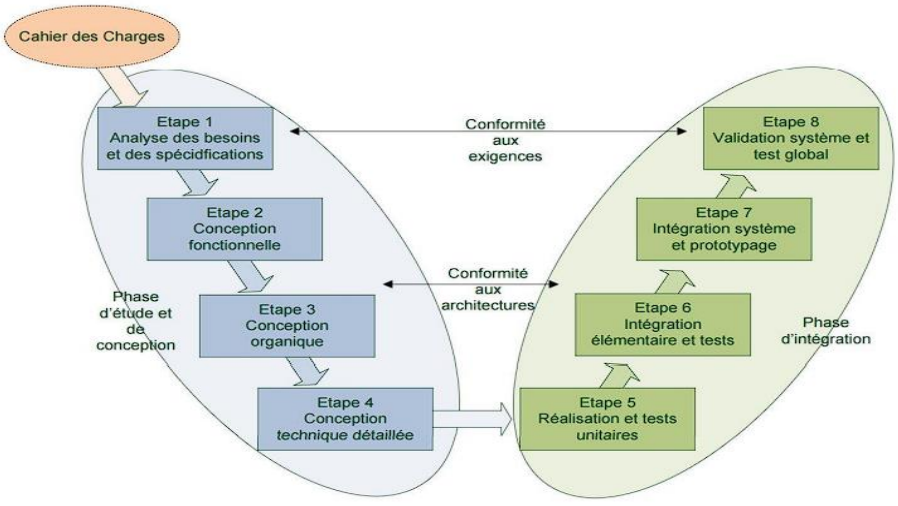


Figure 5 : Méthode en V

Bien que ces méthodes soient simples à comprendre et à mettre en œuvre, elle présente certains limitations telles que la rigidité, le manque de flexibilité, le manque de rétroaction continue etc.

Pour ces raisons, d'autres approches de développement, comme le développement agile, ont gagné en popularité, car elles permettent une plus grande flexibilité et une meilleure adaptation aux changements.

2. Les méthodes agiles

Les méthodologies agiles se caractérisent par l'itération continue, la collaboration et la flexibilité. Les équipes travaillent en cycles courts (itérations) et adaptent constamment le développement en fonction des retours réguliers des parties prenantes **[3]**.

Dans le contexte du développement logiciel, le concept d'agilité se réfère à la capacité des entreprises informatiques à s'ajuster aux besoins évolutifs des clients, souvent exprimés en cours de projet, tout en améliorant la gestion du triptyque « coût/qualité/périmètre fonctionnel » **[4]**.

Nous disposons de plusieurs méthodes agiles, mais pour cette initiative, nous allons nous concentrer principalement sur Scrum et Kanban.

- **Scrum**

Scrum est une méthode de développement agile qui repose sur des itérations courtes et régulières appelées "sprints". Au cours de chaque sprint, une équipe travaille sur un ensemble de fonctionnalités prioritaires, appelées "éléments de backlog", et produit un incrément potentiellement livrable du produit.

Scrum met l'accent sur la transparence, l'inspection et l'adaptation, avec des réunions régulières telles que la planification de sprint, la revue de sprint et la rétrospective de sprint pour favoriser une amélioration continue du processus de développement. Il encourage également le travail en équipe auto-organisée, où les membres de l'équipe collaborent étroitement pour atteindre les objectifs du sprint **[4]**.

La **figure 6** montre le fonctionnement de la méthodologie SCRUM.

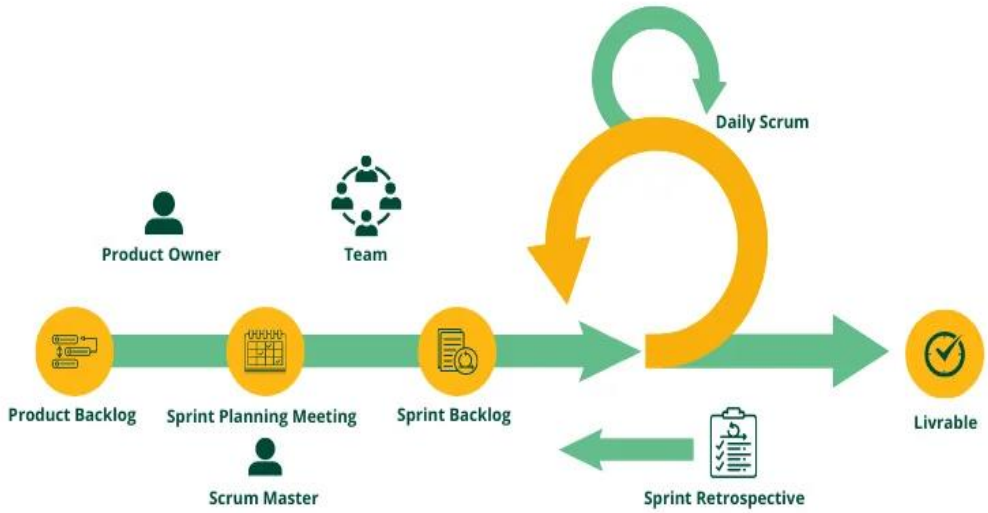


Figure 6 : Framework SCRUM

- **Kanban**

Kanban est une approche agile qui permet d'avoir une représentation visuelle bien plus claire sur l'état d'avancement d'un projet.

Les tâches sont représentées sous forme de cartes et organisées sur un tableau Kanban, généralement divisé en colonnes représentant les différentes étapes du processus.

Le principal objectif de Kanban est d'optimiser le flux de travail, en identifiant et en éliminant les goulets d'étranglement et les gaspillages, tout en minimisant le temps de cycle et en maximisant la valeur livrée **[5]**.

La **figure 7** montre les compositions du tableau Kanban.

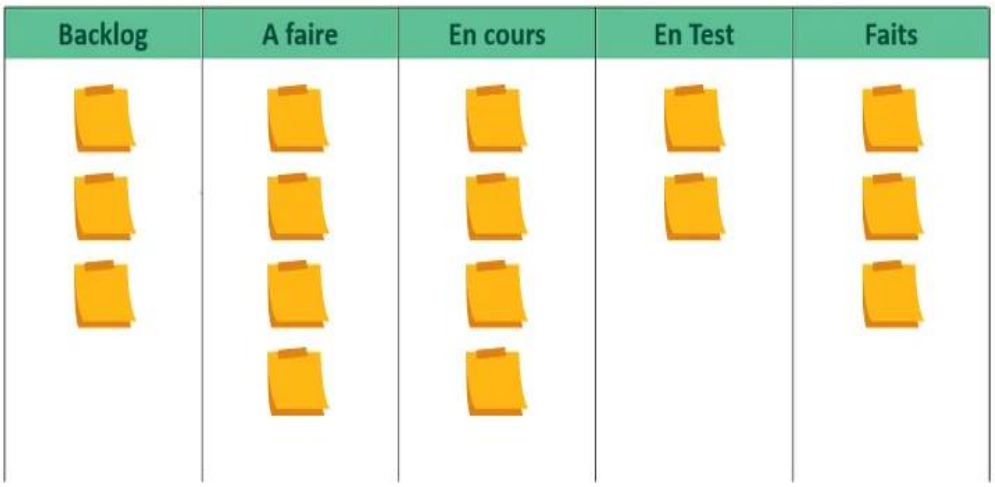


Figure 7 : Tableau KANBAN

3. Etude comparative

L'analyse des méthodologies classiques et agiles permet d'éclairer les choix stratégiques en matière de gestion de projet et de développement logiciel. Le **tableau 1** donne une étude comparative de ces deux approches.

Critères	Méthodologies Classiques	Méthodologies Agiles
Flexibilité au Changement	rigide, difficile à s'adapter aux modifications en cours de projet.	flexible, accueille favorablement les changements tout au long du projet.
Planification	planification exhaustive en amont.	planification itérative, ajustée en fonction des retours réguliers.
Communication	faible interaction client en début de projet.	collaboration continue avec le client et les parties prenantes.
Résultat Final	livré à la fin du cycle de développement.	livraisons fréquentes de versions fonctionnelles tout au long du projet.

Tableau 1 : Comparaison des méthodes classiques et agiles

4. Présentation d'UML

L'Unified Modeling Language (UML) est un langage de modélisation graphique standardisé, composé de diagrammes intégrés qui servent aux développeurs informatiques pour visualiser les objets, les états et les processus au sein d'un logiciel ou d'un système **[6].**

Il offre un ensemble de notations graphiques et de conventions qui facilitent la communication entre les différents intervenants impliqués dans le développement logiciel, que ce soit les concepteurs, les développeurs, ou les responsables de projet.

❖ Objectif de l'UML

UML vise à fournir une méthode systématique pour représenter graphiquement les différents aspects d'un système logiciel. Son objectif est de simplifier la compréhension, la conception, et la documentation des systèmes complexes.

❖ Principaux Concepts d'UML

UML présente un ensemble de concepts fondamentaux tels que **[6]**:

- Diagrammes : UML propose différents types de diagrammes, chacun se concentrant sur un aspect spécifique de la modélisation. Parmi les plus couramment utilisés, on trouve les diagrammes de classe, de séquence, d'activité, de composants, et d'états.
- Classes et Objets : Les diagrammes de classe représentent la structure statique d'un système en mettant en évidence les classes, les attributs, les méthodes et les relations entre les différentes entités.
- Séquences : Les diagrammes de séquence illustrent les interactions entre les objets au fil du temps, mettant en évidence l'ordre chronologique des messages échangés.
- Activités : Les diagrammes d'activité montrent le flux d'activités dans un processus, permettant de visualiser les étapes et les décisions.
- Composants et Déploiement : Ces diagrammes mettent l'accent sur la manière dont les composants logiciels sont organisés et déployés sur un système matériel.
- États : Les diagrammes d'états représentent le comportement d'un objet ou d'un système à différentes étapes.

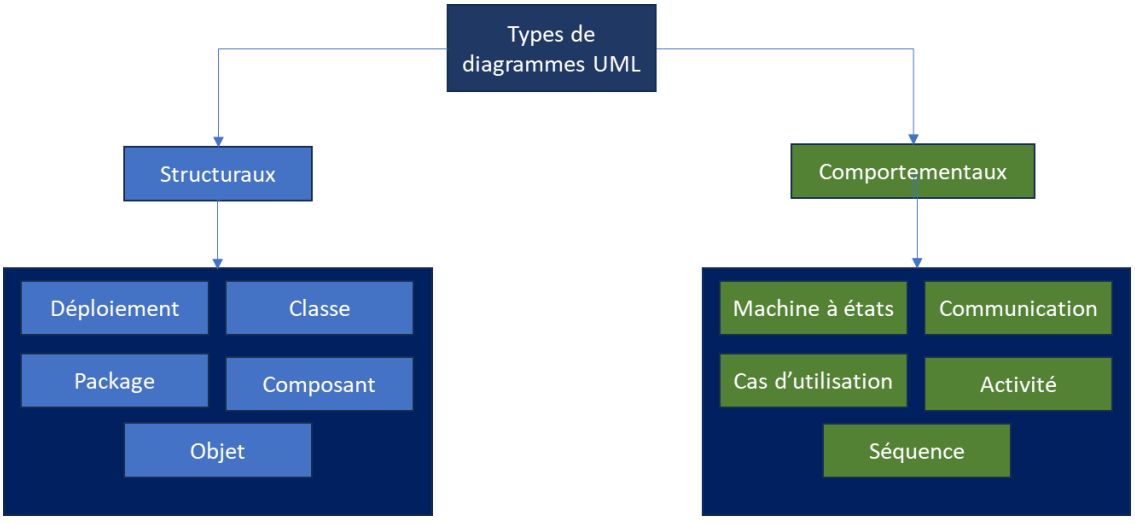


Figure 8 : : Les diagrammes UML

II. Cadre de développement

Les architectures logicielles jouent un rôle crucial dans le développement des applications, et trois approches majeures, à savoir les architectures monolithiques, orientée services (SOA) et en microservices, émergent comme des paradigmes distincts influençant la manière dont les systèmes informatiques sont conçus, déployés et évoluent.

- **Architecture monolithique**

Une application monolithique est un logiciel dans lequel différents composants (tels que l'autorisation, la logique métier, le module de notification, etc.) sont combinés en un seul programme à partir d'une seule plateforme **[7]**.

Ils sont généralement faciles à développer, déployer et tester. Cependant, à mesure que la taille de l'application augmente, il peut devenir plus difficile de maintenir et de faire évoluer le code.

Les différentes parties de l'application partagent la même base de données et communiquent généralement de manière interne.

- **Architecture orientée services**

SOA, ou architecture orientée services, est un modèle d'application où toutes les fonctionnalités sont conçues comme des services autonomes dotés d'interfaces clairement définies, pouvant être invoquées selon des séquences prédéfinies pour constituer des processus d'entreprise **[8]**.

Elle vise à favoriser la réutilisation des services, à simplifier l'intégration des systèmes, à améliorer la flexibilité et l'agilité des entreprises, ainsi qu'à faciliter la gestion des changements.

Les normes telles que SOAP (Simple Object Access Protocol) et REST (Representational State Transfer) sont souvent utilisées pour permettre la communication entre les services dans un environnement SOA.

- **Architecture microservice**

Les microservices sont une approche architecturale où une application est décomposée en un ensemble de services indépendants et autonomes, chacun dédié à une fonctionnalité spécifique **[9]**.

Ils offrent une scalabilité et une flexibilité accrues. Chaque service peut être développé, déployé et mis à l'échelle indépendamment des autres. Cela facilite également la maintenance et la mise à jour des services sans affecter l'ensemble de l'application.

Les microservices communiquent généralement via des API (Interfaces de Programmation d'Applications) ou via des événements et peuvent avoir leur propre base de données

La **figure 9** montre la composition de architectures cités ci-dessus.

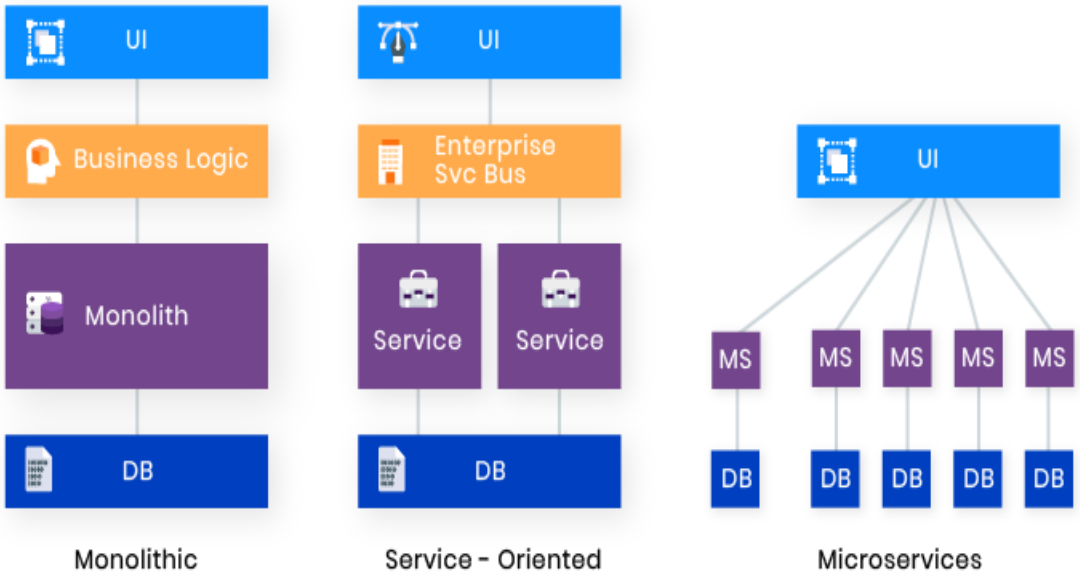


Figure 9 : Architecture monolithique, orienté services et microservice

❖ **Etude comparative**

Dans cette étude comparative, nous explorons les architectures monolithiques, les microservices et l'approche orientée services (SOA), en examinant leurs caractéristiques pour choisir la meilleure approche pour les besoins spécifiques de développement logiciel.

Le **tableau 2** donne une étude comparative des architectures monolithique, orientée services et microservice.

Aspect	**Architecture Monolithique**	**Architecture orientée services**	**Architecture en microservices**
Structure	Application unique fortement couplée.	Multiples services interagissent.	Nombreux petits services indépendants.
Communication	Appels de méthode/fonction directs au sein de l'application.	Communication inter-services via des APIs.	Communication inter-services via des APIs ou des événements.

Aspect	Architecture Monolithique	Architecture orientée services	Architecture en microservices
Scalabilité	Mise à l'échelle de l'application dans son ensemble.	Mise à l'échelle en ajoutant des instances de services spécifiques.	Mise à l'échelle en ajoutant des instances de services individuels.
Flexibilité	Choix technologique limité.	Certaine diversité technologique entre les services distincts.	Grande diversité technologique dans des services isolés.
Aspect	**Architecture Monolithique**	**Architecture orientée services**	**Architecture en microservices**
Déploiement	Unité de déploiement unique.	Déploiement indépendant des services.	Déploiement indépendant des microservices.
Maintenance	Les modifications peuvent impacter l'ensemble de l'application.	Les modifications dans les services ont des effets isolés.	Les modifications dans les microservices ont des effets isolés.
Collaboration d'équipe	L'ensemble de l'équipe travaille sur une seule base de code.	Les équipes collaborent sur des services distincts.	Les équipes collaborent sur des microservices individuels.
Isolation des erreurs	Une seule défaillance peut affecter l'ensemble du système.	Les défaillances sont contenues dans des services spécifiques.	Les défaillances sont contenues dans des microservices individuels.
Gestion de la complexité	Complexité plus élevée en raison de composants fortement couplés.	Complexité modérée avec des services découplés.	Complexité moindre avec des microservices fortement découplés.

Tableau 2 : Comparaison des architectures monolithique, orientée services et microservice

III. Choix retenus : SCRUM et les microservices

1. Justification

La décision d'adopter la méthodologie Scrum et l'architecture basée sur les microservices s'inscrit dans une vision prospective du projet, prenant en considération non seulement les défis immédiats, mais également la nécessité d'anticiper les évolutions futures.

Ces choix se distinguent sur :

- Vision prospective : L'adoption de Scrum et de l'architecture microservices est fondée sur une vision à long terme, visant à accommoder des évolutions futures du projet.
- Facilité d'intégration : La perspective du client, envisageant l'intégration de parties développées par différentes équipes, guide ce choix stratégique pour garantir une facilité d'intégration des futurs modules du projet.

Ces choix méthodologiques et architecturaux apportent une agilité continue, permettant une gestion flexible des exigences changeantes tout au long du cycle de développement. Elles représentent également une stratégie proactive visant à assurer une agilité continue et une intégration harmonieuse des différentes composantes du projet, répondant ainsi pleinement aux attentes du client.

2. Organisation de l'équipe

Le **tableau 3** décrit l'organisation de l'équipe SCRUM pour la réalisation du projet.

Personnes et Fonctions	**Rôles et Description**
Mme Rokhaya Diop : Chargée de projet, Atlantic Digital Solutions	**Scrum Master** : Garant de la méthodologie Scrum. Il veille à ce que les principes et les pratiques Scrum soient respectés.
M Moussa Diop : Directeur Général, Atlantic Digital Solutions	**Product Owner** : Responsable de la définition des besoins du client, de la gestion du carnet de production
M Balla GNINGUE, M Mouhamadou DIAMANKA : Développeurs stagiaires	**Equipe de développement :** professionnels chargés de réaliser le travail du projet.

Tableau 3 : Organisation de l'équipe SCRUM du projet

Conclusion

En conclusion de ce chapitre, nous avons plongé dans l'exploration des deux piliers fondamentaux qui encadrent la réalisation du projet : cadre méthodologique et approche de développement. Notre choix de fusionner ces deux concepts dans notre approche vise à créer un environnement de développement qui transcende les limites traditionnelles, favorisant la

réactivité face aux changements, la garantie de la qualité et la stimulation continue de l'innovation.

Chapitre 3 : Généralités sur les systèmes de contrôle d'accès physique

Introduction

Un système de contrôle d'accès a pour objectif principal de limiter l'accès à certaines ressources (zones, matériels ou informations) à un ensemble de personnes bien définie durant des périodes bien déterminées et de garder la trace des demandes d'accès autorisées ou refusées. Le contrôle d'accès donne à une entité l'autorisation d'accéder aux ressources demandées, qu'elles soient physiques (accès à un bâtiment, une salle, un coffre) ou logiques (accès à certains dossiers, programmes, informations).

I. Définition

Un contrôle d'accès physique est exactement comme son nom l'indique le niveau d'accès donné à l'espace physique ou aux biens physiques d'une entreprise **[10]**.

II. Principaux composants et leurs interactions

La mise en œuvre d'un système de contrôle d'accès physique repose sur divers composants et mécanismes interconnectés visant à réguler l'accès à des zones restreintes.

Ils sont principalement composés de :

- **Lecteurs d'Identification** : Ces dispositifs, tels que les lecteurs de badges RFID ou les lecteurs biométriques, captent les informations d'identification présentées par les utilisateurs.
- **Badges ou Cartes d'Accès** : Les utilisateurs autorisés possèdent des badges, cartes ou dispositifs équivalents contenant des informations d'identification uniques, comme des codes RFID ou des données biométriques.
- **Unité de Traitement et de Contrôle** : L'unité centrale traite les informations reçues des lecteurs et prend des décisions en temps réel sur l'autorisation d'accès.
- **Système de Gestion des Utilisateurs** : La base de données des utilisateurs autorisés est stockée et gérée par un système central qui peut être intégré à d'autres systèmes de gestion.

- **Dispositifs de Verrouillage** :Les mécanismes de verrouillage physiques, tels que des serrures électromagnétiques ou des gâches électriques, sont contrôlés électroniquement pour permettre ou refuser l'accès.

La **figure 10** montre les principaux composants et les interactions d'un système de contrôle d'accès.

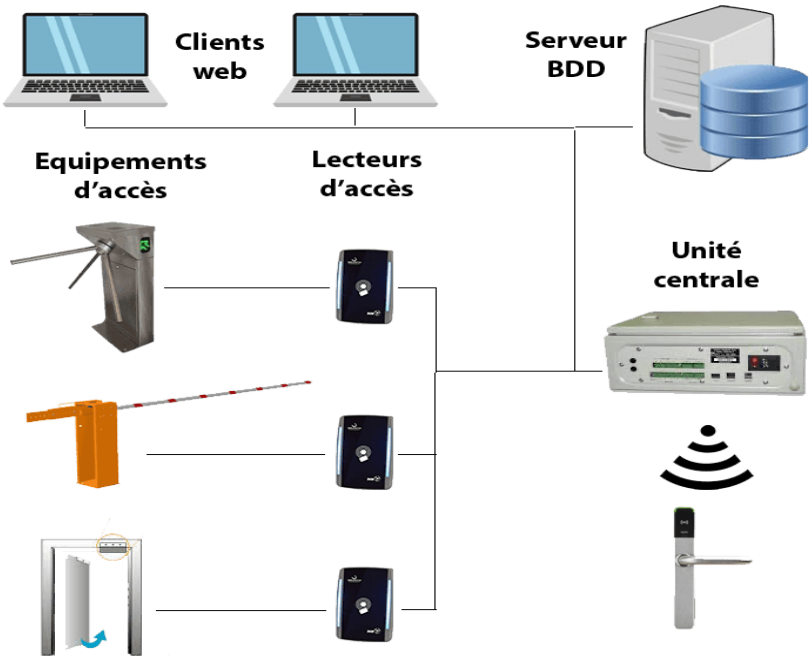


Figure 10 : Composants et interactions d'un système de contrôle d'accès physique

III. Etapes de gestion du contrôle d'accès physique

Au niveau de chaque point de contrôle, l'accès n'est autorisé que si le sujet est porteur d'une autorisation valable (badge, QR code …).

La **figure 11** montre les successions et les étapes de gestion de contrôle d'accès.

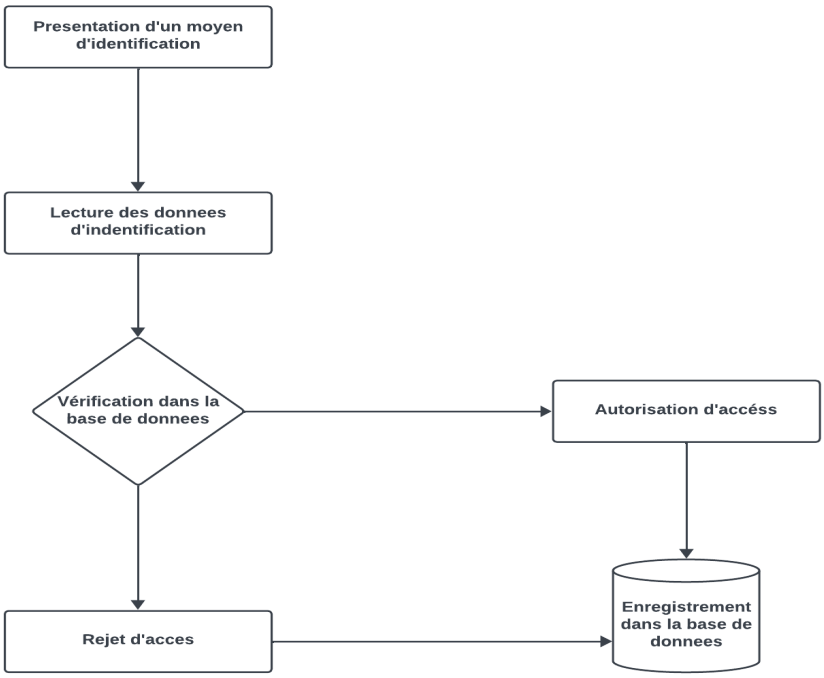


Figure 11: Etapes de contrôle d'accès

IV. Technologies utilisées pour le contrôle d'accès

1. La technologie RFID

L'abréviation RFID signifie « Radio Frequency Identification », en français, « Identification par Radio fréquence ». Cette technologie permet d'identifier un objet, suivre son acheminement et de connaitre sa position dans un environnement interne en temps réel grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet (étiquette RFID) **[11]**.

❖ **Principe**

L'étiquette radiofréquence (transpondeur, étiquette RFID), est composée d'une puce reliée à une antenne, encapsulée dans un support (RFID Tag ou RFID Label).

La puce sert à stocker des données et à les transmettre au lecteur RFID via des ondes radio **[12]**.

Elle est lue par un lecteur qui capte et transmet l'information vers un serveur. On distingue 3 catégories d'étiquettes RFID **[13]** :

- Les étiquettes en lecture seule, non modifiables
- Les étiquettes « écriture une fois, lecture multiple »,
- Les étiquettes en « lecture réécriture ».

Par ailleurs, il existe deux grandes familles d'étiquettes RFID [14] :

- Les étiquettes actives, reliées à une source d'énergie embarquée (pile, batterie, etc.). Les étiquettes actives possèdent une meilleure portée, mais à un coût plus élevé et avec une durée de vie restreinte.
- Les étiquettes passives, utilisant l'énergie propagée à courte distance par le signal radio de l'émetteur. Ces étiquettes à moindre coût sont généralement plus petites et possèdent une durée de vie quasi illimitée. En contrepartie, elles nécessitent une quantité d'énergie non négligeable de la part du lecteur pour pouvoir fonctionner.

❖ Principaux composants et fonctionnement

Un système RFID est composé de deux entités qui communiquent entre elles :

- ❖ Un tag ou étiquette intelligente (aussi appelé transpondeur), associé à l'élément à identifier. Il est capable de répondre à une demande venant d'un lecteur.
- ❖ Une station de base ou lecteur RFID qui a pour mission d'identifier le tag. Le lecteur envoie une onde électromagnétique en direction de l'élément à identifier. En retour, il reçoit l'information renvoyée par le tag **[15]**.

La **figure 12** montre le principe de fonctionnement d'un système RFID

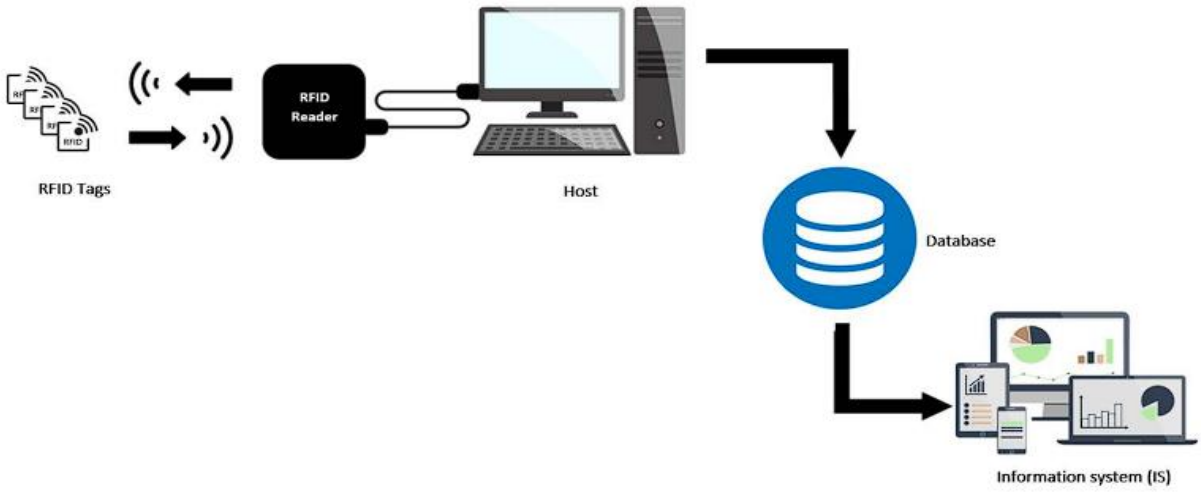


Figure 12 : Principe de fonctionnement d'un tag RFID

2. Technologie de reconnaissance de plaque d'immatriculation

La reconnaissance des plaques d'immatriculation (LPR) est une technologie de pointe qui utilise la vision par ordinateur et l'intelligence artificielle (IA) pour identifier et documenter rapidement les numéros de plaques d'immatriculation des véhicules **[16], [17]**.

❖ Principe

Le principe de la reconnaissance de plaque d'immatriculation, également connue sous le nom de système ANPR, repose sur l'utilisation de technologies telles que des caméras spéciales et des logiciels de traitement d'image pour identifier et interpréter les numéros de plaques d'immatriculation des véhicules **[17], [12]**.

La **figure 13** montre les différents étapes du principe de la reconnaissance de plaque d'immatriculation.

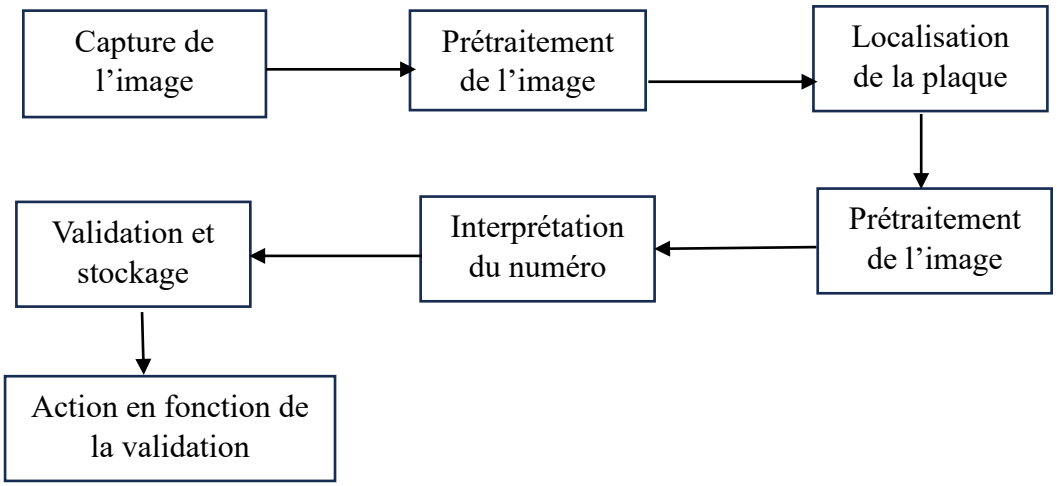


Figure 13 : Principe de la reconnaissance de plaque d'immatriculation

❖ Composants et fonctionnement

Un système de lecture automatique de plaques d'immatriculation se compose principalement de **[18]** :

- Un dispositif caméra
- Un logiciel de reconnaissance de caractères.
- Base de données de plaques d'immatriculation.

Une caméra ANPR positionnée immédiatement derrière la barrière détectera et effectuera la lecture de la plaque d'immatriculation dès l'approche du véhicule. Le numéro de la plaque d'immatriculation est ensuite transmis à la centrale de contrôle d'accès pour validation. En cas

de validation, l'unité de contrôle d'accès émettra un signal d'ouverture à la barrière, permettant ainsi au véhicule d'entrer **[19]**.

La **figure 14** montre le principe de fonctionnement de la reconnaissance de plaque d'immatriculation.

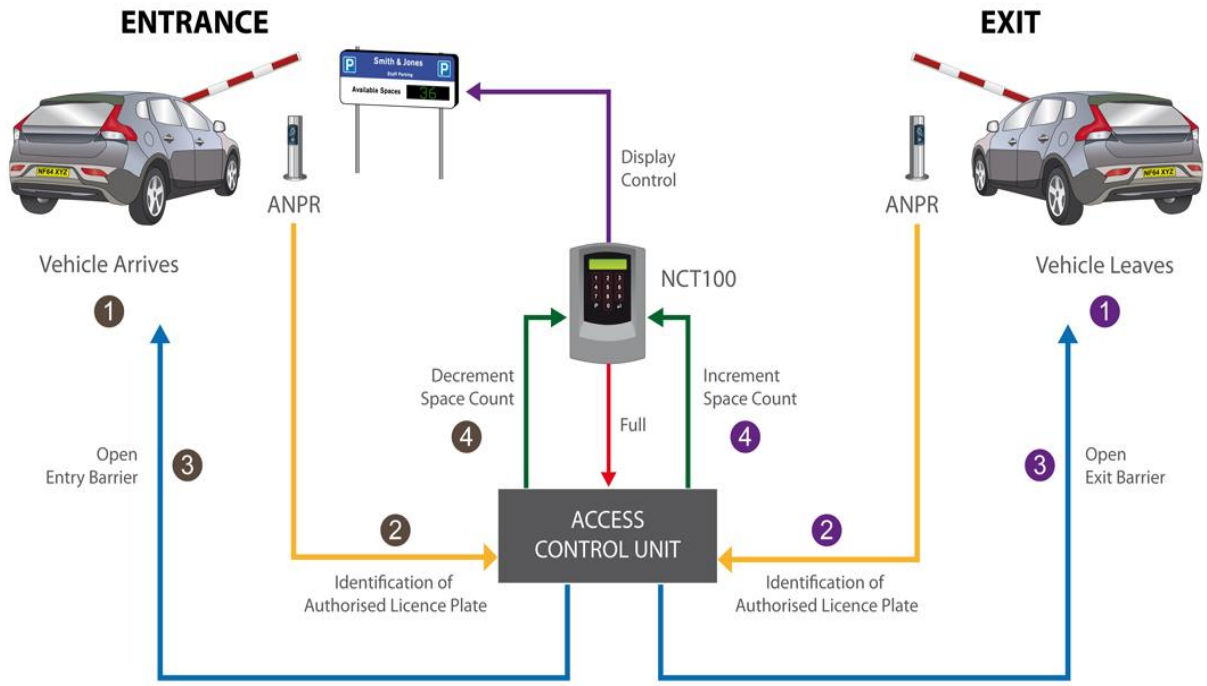


Figure 14 : : Principe de fonctionnement de la reconnaissance de plaque d'immatriculation

3. Reconnaissance Faciale

La technologie de reconnaissance faciale est un système qui identifie la présence d'une personne en analysant une image numérique ou une vidéo de son visage et en la comparant à des données préalablement enregistrées **[20]**.

❖ **Composants et Fonctionnement**

Un système de reconnaissance faciale est principalement composé de :

- **Capteurs d'Image** : Les caméras ou capteurs infrarouges capturent des images du visage de la personne.
- **Unité de Traitement d'Image** : Cette unité traite les images capturées, extrait les caractéristiques du visage et convertit ces informations en données numériques.

- **Base de Données** : Contient les informations biométriques préalablement enregistrées, telles que les caractéristiques faciales ou les modèles de visage associés à des identités spécifiques.
- **Algorithme de Reconnaissance Faciale** : Un ensemble d'algorithmes analyse les caractéristiques du visage capturé et les compare aux données stockées dans la base de données.
- **Système de Gestion** : Un système qui gère les requêtes de reconnaissance, traite les résultats et prend des décisions en fonction des résultats obtenus.

La **figure 15** montre le principe de fonctionnement de la technologie de reconnaissance faciale.

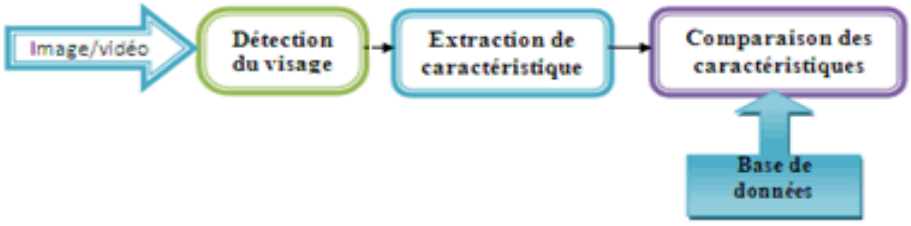


Figure 15 : Principe de fonctionnement de la technologie de la reconnaissance faciale

V. Equipements d'accès

Les dispositifs de contrôle d'accès sont déployés pour réguler le flux de personnes et des véhicules aux points de vérification. Initialement en position fermée, ces dispositifs bloquent l'accès, que ce soit en entrée, en sortie, ou dans les deux sens.

Lorsqu'une demande d'accès est reçue, le système de contrôle examine les données correspondantes dans la base.

Si la demande est autorisée, le mécanisme se déverrouille pour permettre le passage, avec le déblocage électrique du verrou interne pendant une durée définie (paramétrable). Une fois le passage effectué, le dispositif revient à son état initial de blocage.

❖ **Barrière**

La barrière est utilisée pour le control des entrées et/ou sorties des véhicules à un parking, ou aménagements industriels.

❖ **Tourniquet tripode**

Les tourniquets sont équipés d'un mécanisme à bras articulé. Le bras qui se trouve à l'horizontale bloque le passage. Apres rotation d'un-tiers (1/3) de tour du mécanismes le bras tombe en position verticale libérant le passage d'un seul utilisateur.

❖ **Porte pleine hauteur**

Le tourniquet grande hauteur est conçu pour assurer un contrôle d'accès plus sécurisé. Il est destiné particulièrement aux centres sensibles non gardiennés.

VI. Etude comparative

La **tableau 4** suivant définit une étude comparative entre les technologies de contrôle d'accès listées plus haut.

Critères	**RFID**	**Reconnaissance Faciale**	**Reconnaissance de Plaque d'immatriculation**
Principe de Fonctionnement	Transmission RF d'informations	Analyse des caractéristiques du visage	Capture et analyse des caractères de la plaque
Niveaux de Sécurité	Vulnérabilité aux clonages, accès à distance non autorisé	Niveau élevé avec risque d'erreurs de reconnaissance	Sécurité élevée, risque de dupliquer certaines plaques
Coût et Complexité	Coût relativement bas, infrastructure peut être complexe	Coûts variables, complexes	Coûts intermédiaires, systèmes souvent plus simples à déployer
Applicable sur personnes	Oui	Oui	Non
Applicable sur véhicules	Oui	Non	Oui

Tableau 4 : Comparaison des technologies RFID, reconnaissance de plaque et faciale

VII. Choix retenu : RFID

Le choix de la technologie RFID a été judicieusement effectué en considération de plusieurs critères clés.

En ce qui concerne les coûts et la complexité, le choix de RFID s'est avéré pertinent avec ses coûts relativement bas, même si l'infrastructure peut être complexe, particulièrement pour les systèmes étendus. Cela a été préféré par rapport à la reconnaissance faciale, qui implique des coûts variables et une complexité accrue dans la configuration du système.

L'applicabilité sur des personnes et des véhicules a été un facteur clé dans la décision. RFID s'est distingué en étant applicable aussi bien sur des personnes que sur des véhicules, offrant ainsi une solution polyvalente adaptée au contrôle d'accès.

Cette caractéristique polyvalente a été privilégiée par rapport à la reconnaissance faciale, principalement applicable sur des individus, et à la reconnaissance de plaque d'immatriculation, qui se concentre davantage sur les véhicules.

Conclusion

En conclusion de ce chapitre, il apparaît que les dispositifs de contrôle d'accès jouent un rôle crucial dans la sécurisation des espaces et la gestion des flux de personnes et de véhicules. Nous avons exploré diverses technologies, parmi lesquelles la RFID, la reconnaissance faciale et la reconnaissance de plaque d'immatriculation, chacune présentant des avantages et des limites spécifiques. Suite à une compréhension des besoins spécifiques et à une étude comparative, le choix est orienté vers les technologies RFID.

Chapitre 4 : Spécifications et Analyse des besoins

Introduction

Au cours de cette phase, nous approfondirons notre compréhension des spécificités de l'environnement portuaire pour définir de manière précise les besoins et les exigences propres à ce contexte singulier. Nous avons procédé à l'identification minutieuse des modules du système, des acteurs impliqués, ainsi que des fonctionnalités principales. La description de quelques cas d'utilisation et les diagrammes séquentiels et d'activité correspondants ont été employés de manière illustrative pour rendre compte visuellement de cette analyse et spécification des besoins.

I. Spécifications des besoins

1. Identification des modules

Le **tableau 5** décrit les principaux modules qui composent le système.

Modules de gestion	**Description**
De badges et profils d'accès	• Gérer (attribuer, activer, désactiver) les badges d'accès • Gérer (créer, modifier, supprimer) un profil d'accès pour chaque groupe d'utilisateurs.
De contrôle d'accès	• Octroyer les autorisations d'accès • Visualiser les entrées et les sorties • Contrôler barrière
Des sociétés	• Gérer (créer, modifier, supprimer) une société locataire • Ajouter un responsable à chaque société
Des ressources	• Gérer (ajouter, modifier, supprimer, lister) les employés de la société. • Gérer (ajouter, modifier, supprimer, lister) les véhicules de la société. • Demander des badges d'accès
Des statistiques	• Visualiser entrées et sorties (entrée), disponibilité des espaces, les visites des sociétés externes.

Des notifications	• Recevoir les notifications sur les activités de la plateforme (entrée, sortie, tentative d'intrusion, demande et octroi d'autorisation d'accès etc.)

Tableau 5 : Les modules du systèmes

2. Identifications des acteurs

Un acteur est l'archétype de l'utilisateur (personne, processus externe, …) qui interagit avec le système. Par défaut, c'est un acteur principal, c'est-à-dire qu'il agit directement sur le système et en attend des résultats ou biens, il peut être un acteur secondaire qui est souvent sollicité pour des informations supplémentaires.

Le **tableau 6** montre les acteurs identifiés et les modules auxquelles ils ont accès.

Acteurs	Modules
Administrateur du système	• Gestion des badges et profils d'accès • Gestion des sociétés • De contrôle d'accès • De statistiques • Des notifications
Responsable de société	• Gestion des ressources (Personnel et véhicule) • De statistiques • Des notifications
Responsable de GIE	• Gestion des ressources (Personnel) • De statistiques • Des notifications

Tableau 6 : Les acteurs du système

3. Fonctionnalités du système de contrôle d'accès

Le **tableau 7** décrit les fonctionnalités majeures que le système de contrôle d'accès offre.

Fonctionnalités	Description
Gestion des sociétés et des ressources (personnels et véhicule)	Centralisation de la gestion des sociétés et de leur ressource (personnel et véhicule), permettant de superviser toutes les informations essentielles associées à chaque société.
Gestion des espaces de stationnement	Allocation dynamique des places de stationnement en fonction des sociétés locataires et de leurs besoins, tout en maintenant une mise à jour constante du nombre de places disponibles et occupées.
Profils d'accès	Création de profils d'accès personnalisés pour la validité des badges d'accès.
Gestions des badges d'accès	Demande et attribution de badges aux personnels ou aux véhicules des sociétés locataires ou GIE en fonction des profils d'accès
Contrôle d'accès	Gestion automatisée des accès, assurant ainsi que seuls les véhicules et les individus autorisés puissent entrer dans la plateforme de distribution, et de garantir un contrôle précis sur les autorisations d'accès.
Notifications entrées/sorties	Notifications instantanées aux sociétés locataires de la plateforme ainsi qu'aux autres parties concernées chaque fois qu'un véhicule ou un individu entre ou quitte la plateforme.

Tableau 7 : Les principales fonctionnalités du système

4. Diagrammes de cas d'utilisation

a. Diagramme de cas d'utilisation de l'administrateur

Le diagramme de cas d'utilisation de l'administrateur nous permet de représenter l'ensemble des fonctionnalités auxquelles a accès l'administrateur.

La **figure 16** montre le diagramme de cas d'utilisation de l'administrateur du système.

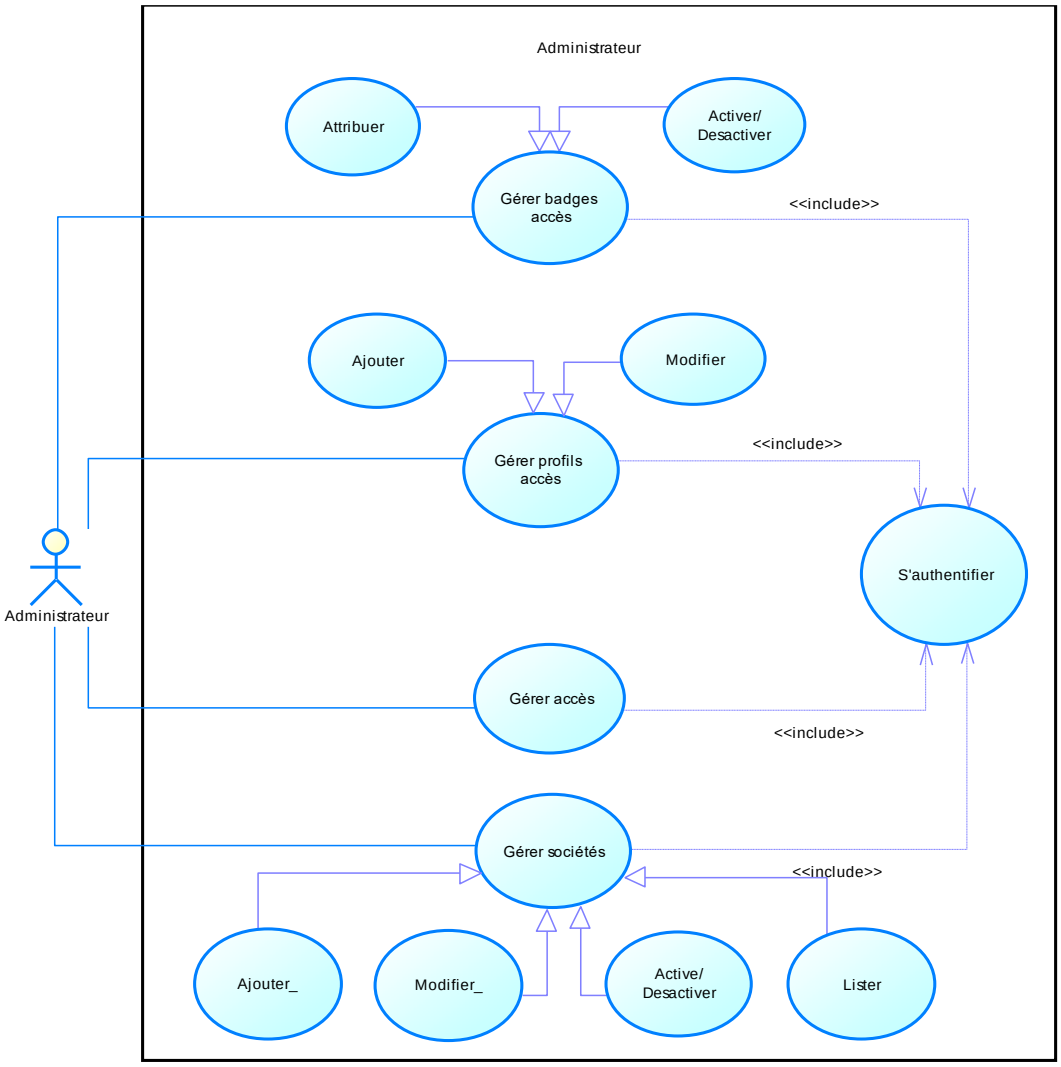


Figure 16 : Diagramme de cas d'utilisation de l'administrateur

b. Diagramme de cas d'utilisation de responsable de société

Le diagramme de cas d'utilisation de responsable de société nous permet de représenter l'ensemble des fonctionnalités dont a accès chaque responsable de société.

La **figure 17** montre le diagramme de cas d'utilisation des responsables de société.

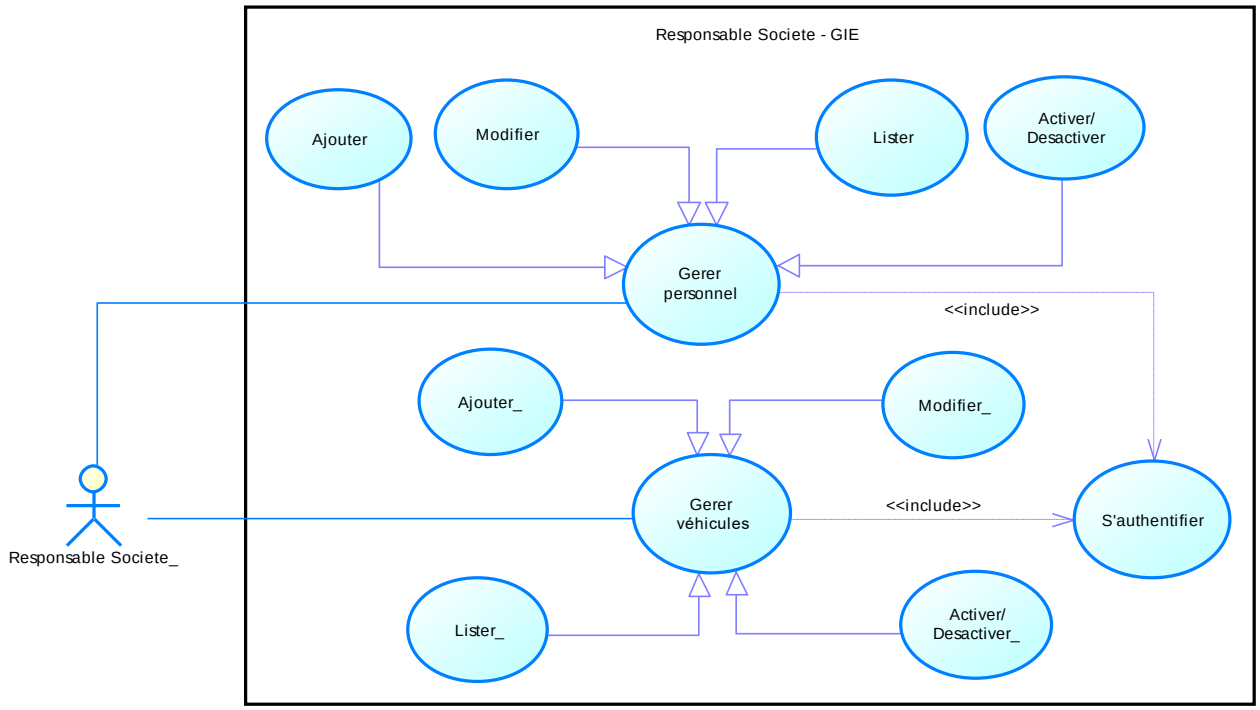


Figure 17 : Diagramme de cas d'utilisation de responsable de société

c. Diagramme de cas d'utilisation de responsable de GIE

Le diagramme de cas d'utilisation de responsable de GIE nous permet de représenter l'ensemble des fonctionnalités dont a accès chaque responsable de GIE.

La **figure 18** suivante montre le diagramme de cas d'utilisation du responsable de chaque GIE

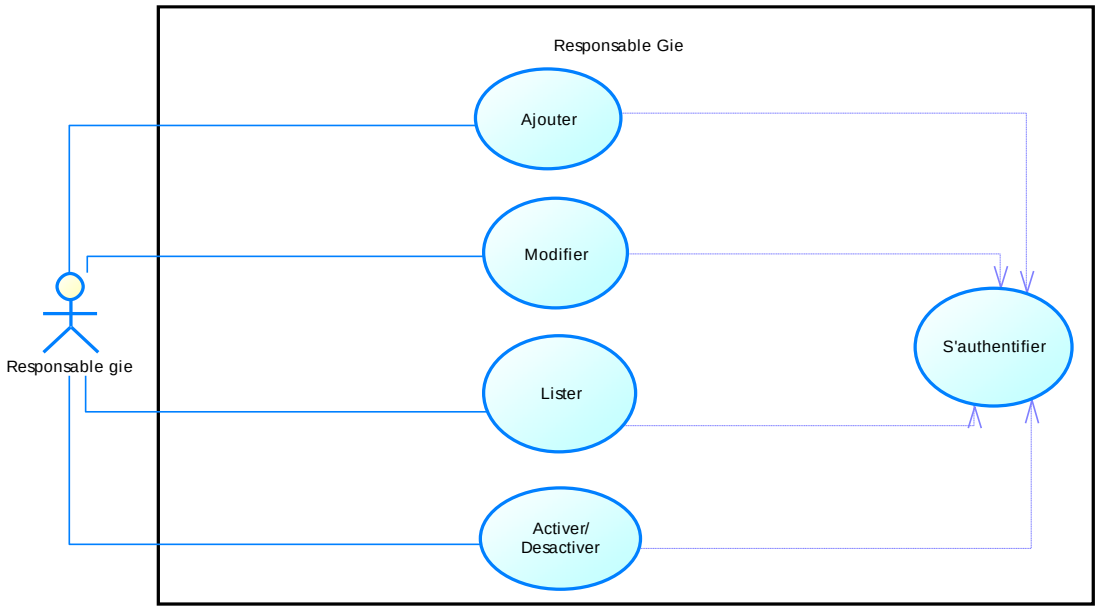


Figure 18 : Diagramme de cas d'utilisation du responsable de GIE

II. Analyse des besoins

1. Besoins fonctionnels

a. Authentification

Ce cas d'utilisation concerne l'authentification des utilisateurs du système notamment l'administrateur, les responsables société de la plateforme de distribution et les responsables des GIE. L'utilisateur doit être authentifié avant d'accéder au système.

Le **tableau 8** décrit le cas d'utilisation de l'authentification.

Nom	Authentification
Acteurs	Administrateur, responsable de société, responsable de GIE
Résumé	Vérification de l'identité de l'utilisateur
Précondition	L'utilisateur doit être en possession d'informations d'accès ou d'un identifiant valide
Scénario nominal	• L'utilisateur renseigne son login et son mot de passe. • Le système autorise l'accès.
Post-condition	L'utilisateur est authentifié et accède aux fonctionnalités du système
Exception	Si l'utilisateur renseigne des informations de connexion invalides, l'accès est refusé.

Tableau 8 : Description du cas d'utilisation de l'authentification

i. Diagramme de séquence

Le diagramme ci-dessous décrit le scénario normal cité ci-dessus pour l'authentification des utilisateurs du systèmes tels que l'administrateur du système, le responsable de chaque société et le responsable de chaque GIE

La **figure 19** suivante décrit le diagramme de séquence associé à l'authentification.

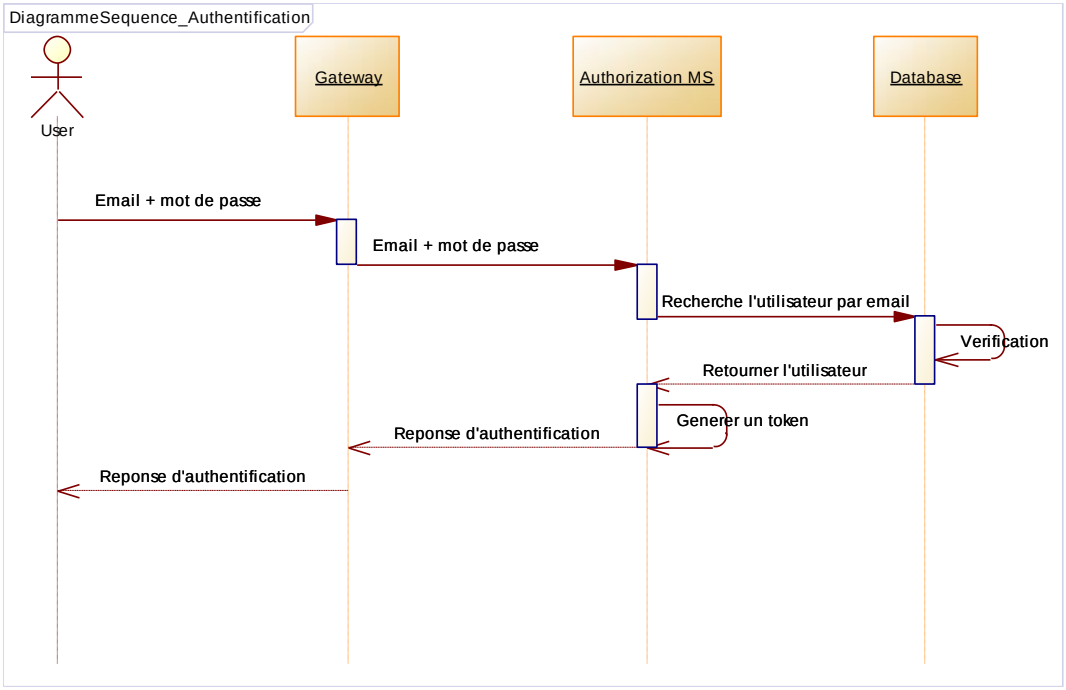


Figure 19 : Diagramme de séquence du cas d'utilisation Authentification

ii. Diagramme d'activité

La **figure 20** décrit le diagramme d'activité du scénarii nominal lors de l'authentification des utilisateurs du système.

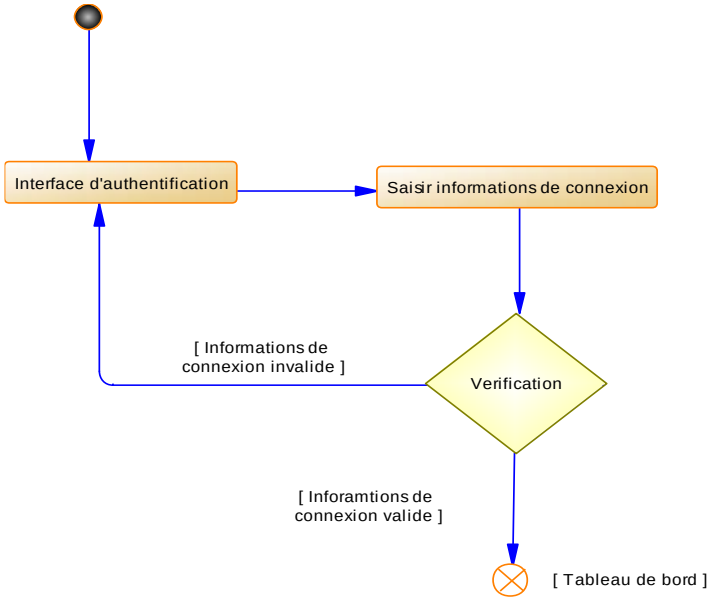


Figure 20 : Diagramme de séquence de l'authentification

b. Contrôle d'accès des employés et des camions des sociétés internes

Ce cas d'utilisation concerne le contrôle d'accès des employés et des camions des sociétés internes entrant dans la plateforme de distribution. Le système doit vérifier les autorisations d'accès de la personne ou du véhicule.

Le **tableau 9** décrit le cas d'utilisation du contrôle d'accès des employés et des camions.

Nom	Contrôle d'accès des employés et des camions des sociétés internes
Acteur	Système de contrôle d'accès
Résumé	Gestion de l'entrée ou de la sortie des employés et des camions des sociétés internes dans la plateforme de distribution
Précondition	• Les employés ou les camions doivent être en possession d'un identifiant valide.
Scénario nominal	• L'employé ou le conducteur approche le point d'entrée ou de sortie du système de contrôle d'accès. • L'employé ou le conducteur présente l'identifiant. • Le système vérifie l'authenticité de l'identifiant. • L'employé ou le camion est autorisé à entrer ou à sortir de la plateforme de distribution.
Post-condition	La personne ou le véhicule est autorisé à entrer ou à sortir de la plateforme
Exceptions	• Si l'employé ou le conducteur présente un identifiant invalide, l'accès est refusé. • Si le nombre de place alloué à la société concernée est atteint, l'accès du camion est refusé

Tableau 9 : Description du cas d'utilisation de contrôle d'accès des employés et des camions des sociétés internes

i. Diagramme de séquence

La **figure 21** montre le diagramme de séquence du scénario normal cité ci-dessus pour le contrôle d'accès des employés et des camions des sociétés internes.

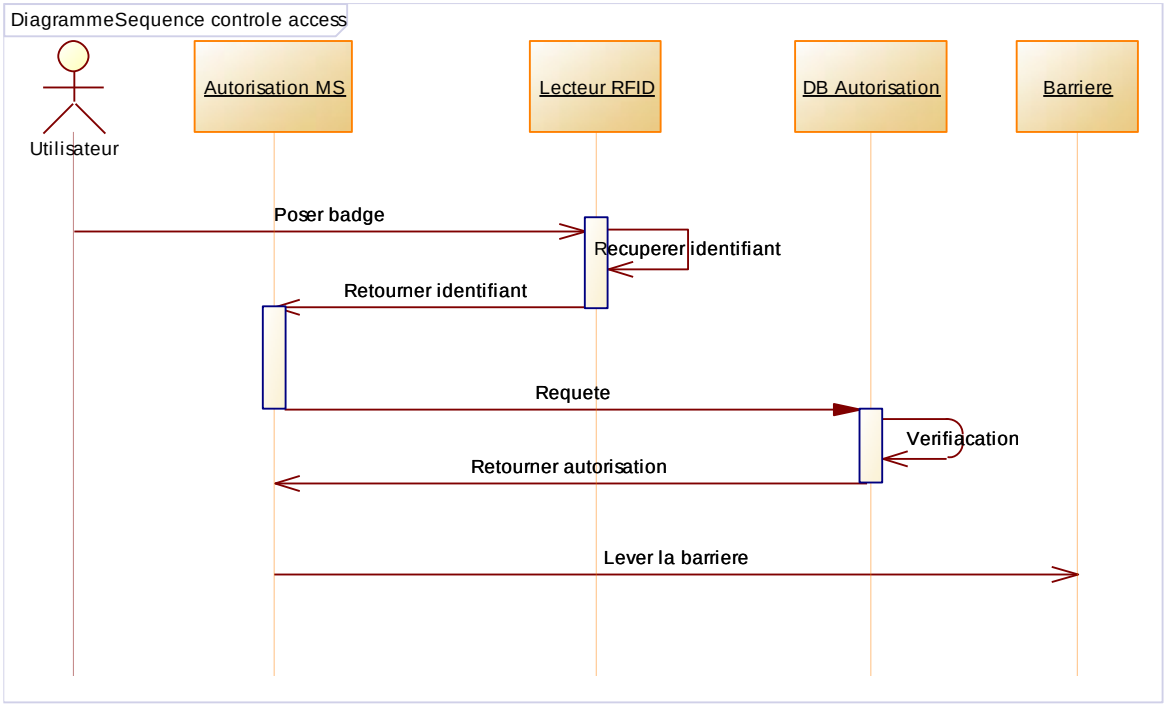


Figure 21 : Diagramme de séquence pour le cas d'utilisation de contrôle d'accès des employés et des camions des sociétés internes

ii. Diagramme d'activité

La **figure 22** montre le diagramme d'activité du scénario normal cité ci-dessus lors du contrôle d'accès des employés et des camions des sociétés internes.

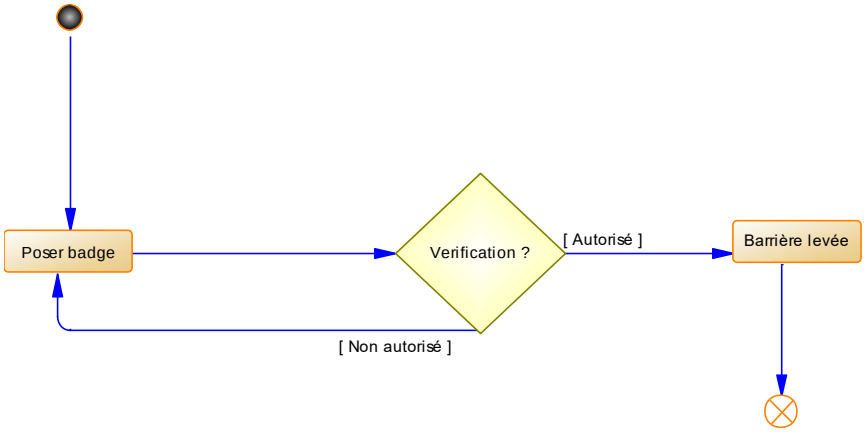


Figure 22 : Diagramme d'activité pour le cas d'utilisation de contrôle d'accès des employés et des camions des sociétés internes

c. Attribution de badges

Ce cas d'utilisation concerne l'attribution de badges d'accès aux employés des sociétés implantées au sein de la plateforme. Le responsable de la société fait la demande des badges d'accès auprès de de l'administrateur.

Le **tableau 10** décrit le cas d'utilisation de l'attribution de badges.

Nom	Attribution de badges d'accès
Acteur	Administrateur du système
Résumé	Attribution de badges d'accès aux employés et des camions des sociétés implantées, aux manœuvres des GIE dans la plateforme respectivement sous la demande du responsable de la société et du responsable du GIE
Précondition	Une demande de badges d'accès a été soumise
Scénario nominal	• Le responsable de société ou responsable de GIE soumet une demande de badge d'accès. • L'Administrateur vérifie les informations de l'employé, du manœuvre ou du camion • L'administrateur octroie un badge à l'entité correspondante
Post-condition	L'employé ou le manœuvre reçoit le badge, et peut l'utiliser pour accéder à la plateforme .
Exceptions	• Les informations de l'employé ou du manœuvre sont erronés ou demande mal soumise.

Tableau 10 : Description du cas d'utilisation de l'attribution de badges

i. Diagramme de séquence

La **figure 23** montre le diagramme de séquence du scénario normal pour l'attribution de badge à un employé ou à un camion d'une société locataire.

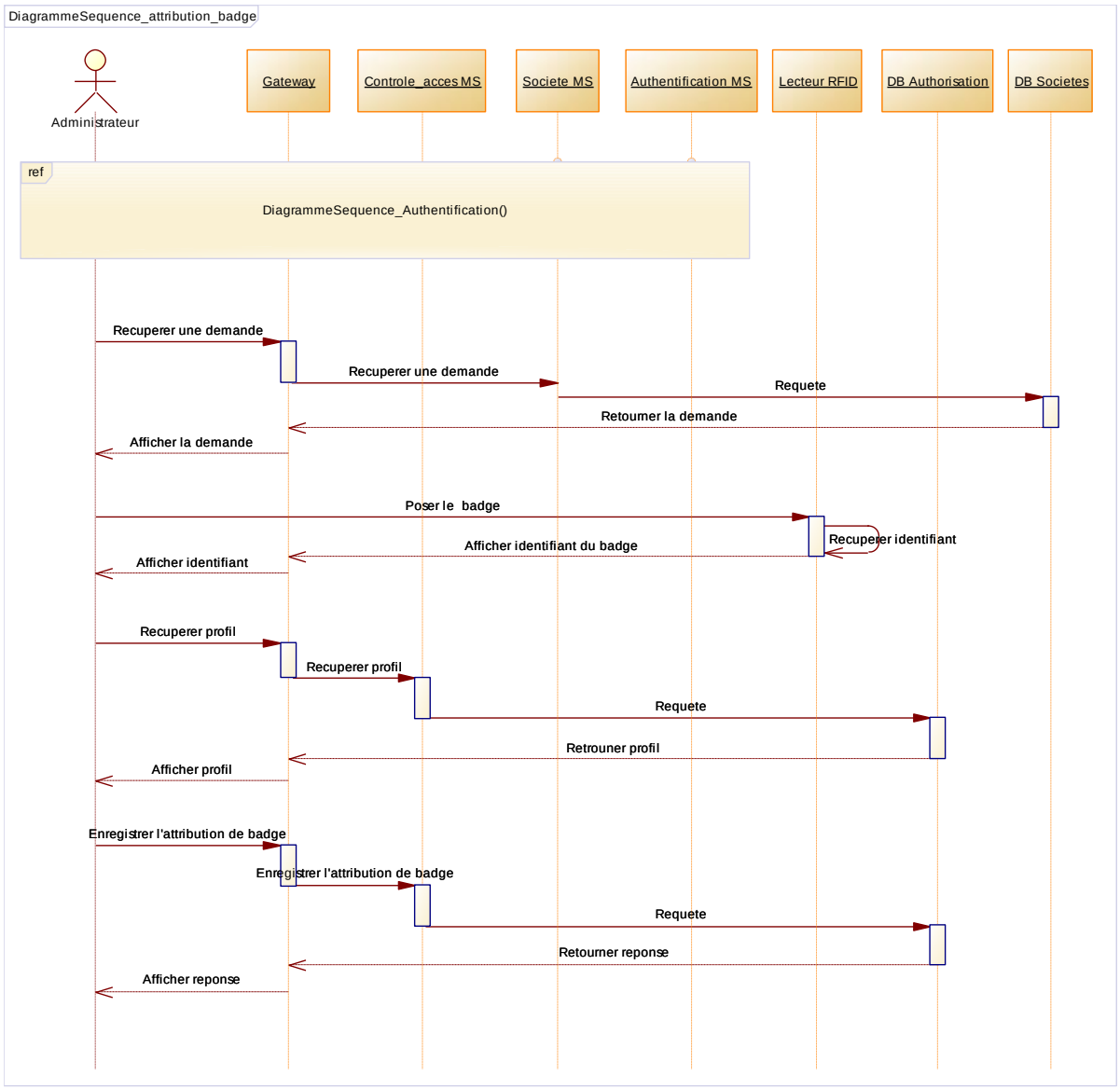


Figure 23 : Diagramme de séquence pour l'attribution de badges

ii. Diagramme d'activité

La **figure 24** montre le diagramme de d'activité du scénario normal pour l'attribution de badge à un employé ou à un camion d'une société locataire.

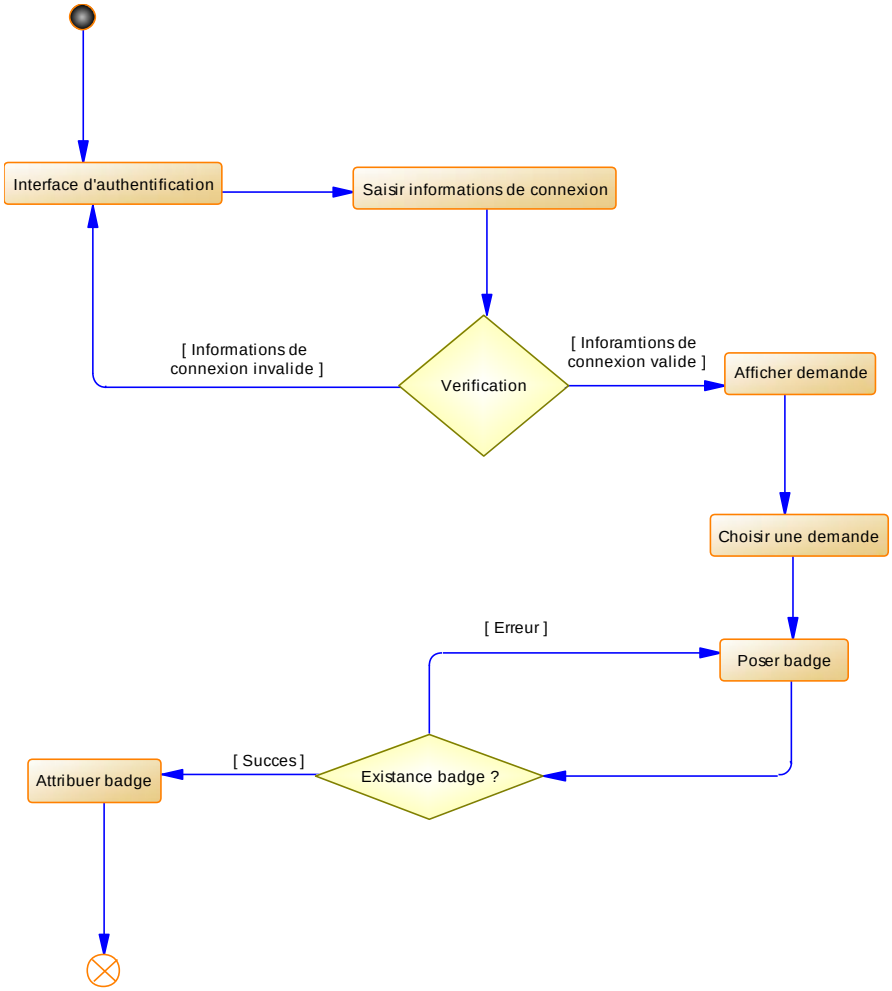


Figure 24 : Diagramme d'activité pour l'attribution de badges

2. Besoins non fonctionnels

Les besoins non fonctionnels définissent des restrictions et des contraintes impactant le service du système, incluant des considérations environnementales, d'implémentation, de performances, de dépendances projet, de facilité de maintenance, d'extensibilité et de fiabilité. Pour ce projet, l'application doit satisfaire les exigences suivantes :

- **Sécurité** : Garantir un haut niveau de sécurité par la prévention des accès non autorisés, l'implémentation de mécanismes de protection des données, de cryptage et d'authentification pour assurer la confidentialité et l'intégrité des informations sensibles.

- **Disponibilité** : Maintenir une disponibilité élevée pour assurer un accès constant à la plateforme, avec des temps d'indisponibilité minimisés pour éviter les perturbations dans les opérations logistiques.
- **Performances** : Gérer efficacement un grand nombre d'utilisateurs et de véhicules tout en maintenant des temps de réponse rapides et efficaces.
- **Scalabilité** : Être évolutif pour s'adapter à l'augmentation du nombre d'utilisateurs et de sociétés locataires sans compromettre les performances.
- **Traçabilité** : Enregistrer de manière précise et complète toutes les activités d'accès pour permettre une traçabilité complète des opérations.
- **Convivialité** : Offrir une interface utilisateur conviviale et intuitive pour faciliter la gestion des accès pour l'administrateur et les responsables de société.
- **Séparation des responsabilités** : Garantir une séparation claire des responsabilités entre l'administrateur et les responsables de société pour éviter tout conflit d'intérêts ou d'accès non autorisés.
- **Audibilité** : Permettre un suivi détaillé des activités d'accès pour faciliter les audits de sécurité et la détection des comportements suspects.
- **Conformité aux normes** : Respecter les normes de sécurité, de confidentialité et de gestion des données en vigueur, notamment en matière de protection des informations personnelles et sensibles.
- **Guide d'utilisation** : Être accompagné d'un guide détaillé expliquant comment les utilisateurs doivent interagir avec le système, couvrant l'enregistrement, la gestion des autorisations et la consultation des rapports.
- **Guide d'administration** : Être accompagné d'un guide d'administration détaillant la gestion des comptes d'utilisateurs, les autorisations, les journaux d'accès, etc.
- **Guide de maintenance** : Être accompagné d'un guide de maintenance pour les opérations planifiées, les mises à jour logicielles et les sauvegardes régulières.

Ces besoins non fonctionnels sont cruciaux pour assurer le bon fonctionnement, la sécurité et l'efficacité du système de contrôle d'accès dans la plateforme de distribution, tout en offrant une expérience utilisateur optimale.

Conclusion

En conclusion de cette phase de spécifications et d'analyse des besoins, nous avons approfondi notre compréhension des spécificités de l'environnement portuaire afin de définir de manière précise les besoins et les exigences propres à ce contexte singulier. L'identification minutieuse

des modules du système, des acteurs impliqués, ainsi que des fonctionnalités principales a été menée avec rigueur.

Les prochaine étape consistera à la conception, en veillant à ce que chaque composant contribue de manière cohérente à l'objectif global du système de contrôle d'accès.

Chapitre 5 : Conception du Système

Introduction

Dans le processus de conception du système de contrôle d'accès, notre orientation se dirige résolument vers la création d'une solution sur mesure. Nous allons approfondir cette approche en soulignant la flexibilité et la capacité de répondre de manière précise à nos besoins spécifiques. L'objectif de ce chapitre est d'apporter une clarté supplémentaire sur notre démarche dans la réalisation d'un système de contrôle d'accès, finement adapté aux exigences particulières de ce projet.

I. Conception générale du système

1. Architecture logicielle du système

Dans l'architecture du système utilisant des microservices pour la plateforme de distribution, l'ajout de certains services essentiels pour le bon fonctionnement de l'ensemble peut être envisagé :

- **Service de Configuration**
  - Ce module a pour objectif de centraliser la configuration des divers microservices.
  - Il facilite la gestion et la distribution uniforme des paramètres de configuration à travers l'intégralité du système.
  - Il garantit la souplesse nécessaire pour ajuster les configurations sans nécessiter des modifications directes sur chaque microservice individuel.
- **Service de Découverte**
  - Ce composant revêt une importance cruciale en permettant une découverte dynamique des microservices actifs au sein du système.
  - L'utilisation de mécanismes tels que les registres et la résolution de noms facilite la localisation et l'accès aux microservices actifs.
  - Il favorise la scalabilité et la maintenance en autorisant l'ajout ou la suppression dynamique de microservices sans perturber d'autres composants du système.
- **Service de Proxy**
  - Fonctionnant comme une interface unifiée, ce service agit en tant que passerelle centrale pour accéder aux différents microservices.

- Il dirige les requêtes des clients vers les microservices appropriés, tout en assurant la sécurité par l'application de politiques d'authentification et de contrôle d'accès avant de rediriger les requêtes.

Parmi les modules de gestion nous avons :

- **Gestion des sociétés et des ressources**
  - Ce module permet la gestion des sociétés au sein de la plateforme de distribution, incluant l'enregistrement du personnel et des véhicules.
  - Il surveille la disponibilité des places dans les locaux des sociétés internes.
- **Gestion des badges et profils d'accès**
  - Ce module facilite la demande et l'attribution des badges d'accès pour le personnel et les véhicules des sociétés internes.
  - Il supervise l'émission et la révocation des badges d'accès permanents et temporaires, tout en gérant les profils d'accès et les informations personnelles associées.
- **Gestion des contrôles d'accès**
  - Ce composant permet d'attribuer des autorisations d'accès au personnel et aux véhicules des sociétés.
  - Il contrôle les barrières d'accès, permettant d'ordonner leur ouverture ou fermeture.
- **Gestion des notifications**
  - Ce composant centralise la logique pour créer et distribuer des notifications à diverses parties prenantes, comme les responsable des sociétés locataires, des GIE et l'administrateur du système.
  - Elle personnalise le contenu des notifications en fonction des besoins, par exemple, en générant des alertes sur les places disponibles, des rappels de rendez-vous, ou des mises à jour sur les changements d'autorisations d'accès.
- **Gestion des mails**
  - Le service d'envoi de mails centralise la logique pour notifier les parties concernées suite à des actions telles que l'ajout d'un nouvel employé, d'un nouvelle camion etc.

Nous avons également des services de supervisons et de traçage :

- **Service de supervision**
  - **Spring-boot Admin :** il fournit une interface d'administration pour la gestion et la surveillance des applications Spring Boot. Il offre également des fonctionnalités

telles que l'état de l'application, les vérifications de santé, les métriques, les propriétés d'environnement, et la possibilité de gérer et interagir avec les applications Spring Boot.

- **Prometheus :** il s'agit d'une boîte à outils de surveillance et d'alerte open source conçue pour la fiabilité et la scalabilité. Il collecte et stocke des données de séries chronologiques, offre des capacités de requête puissantes via PromQL, et peut être intégré à divers exportateurs pour recueillir des métriques à partir de différents services.
- **Grafana :** C'est Plateforme d'analyse et de surveillance open source qui s'intègre à diverses sources de données, y compris Prometheus, pour créer des tableaux de bord visuellement attrayants et personnalisables. Il permet de créer et de partager des tableaux de bord interactifs avec une large gamme de visualisations de données, en faisant un excellent outil pour la surveillance et l'analyse.

❖ **Service de traçage**

- **Zipkin :** C'est un système de traçage distribué qui aide à collecter, analyser et visualiser des traces de requêtes à mesure qu'elles traversent un système distribué.
  Il permet de suivre le flux des requêtes à travers les microservices, facilitant l'identification des goulots d'étranglement de performance et la compréhension des interactions entre différents composants.

La **figure 25** suivante monte l'architecture résultante mise en place.

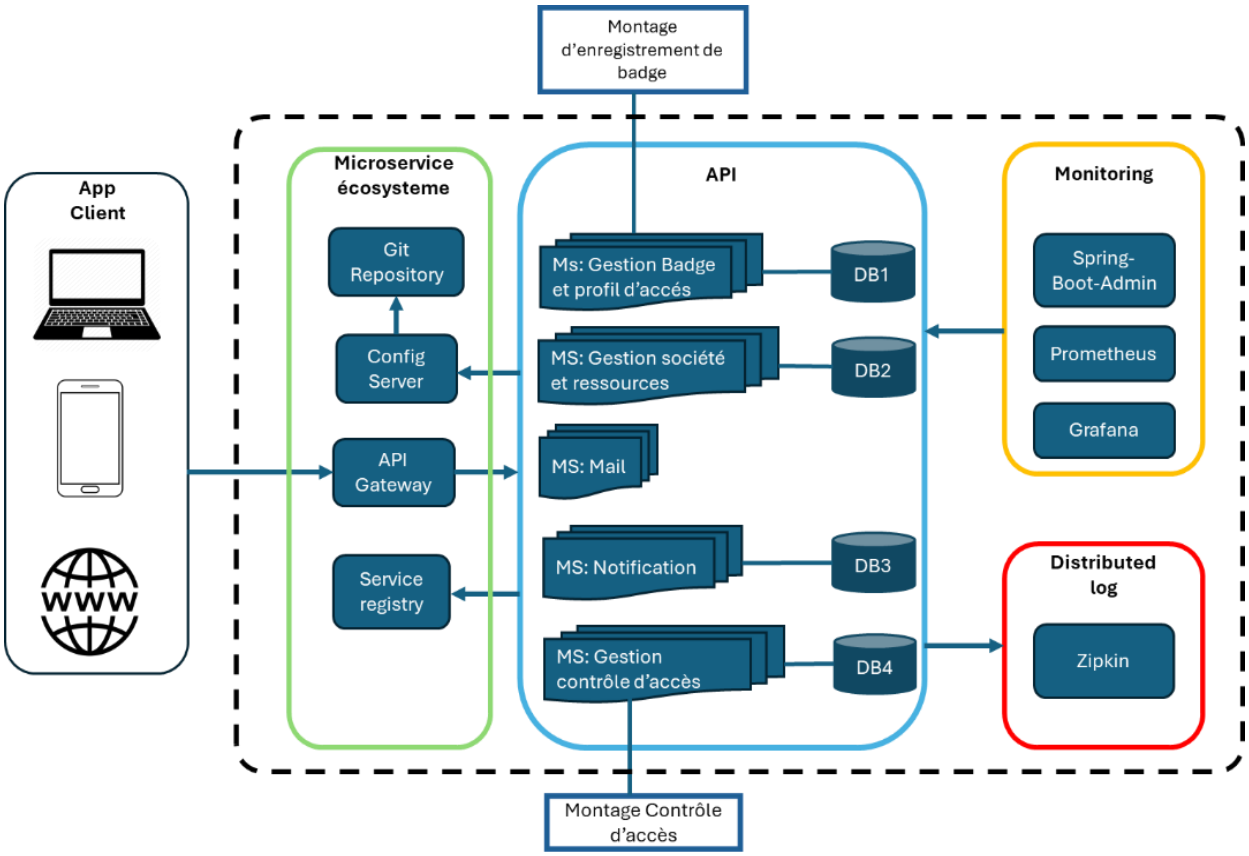


Figure 25 : Architecture générale du système

2. Diagramme de composants

Ce diagramme offre une illustration claire de l'organisation des composants logiciels, de leurs interactions et de leurs dépendances mutuelles pour assurer le bon fonctionnement de notre système. Il permet de visualiser de manière concise la structure interne du système, facilitant ainsi la compréhension des relations entre les différents éléments logiciels.

La **figure 26** montre le diagramme de composants du système.

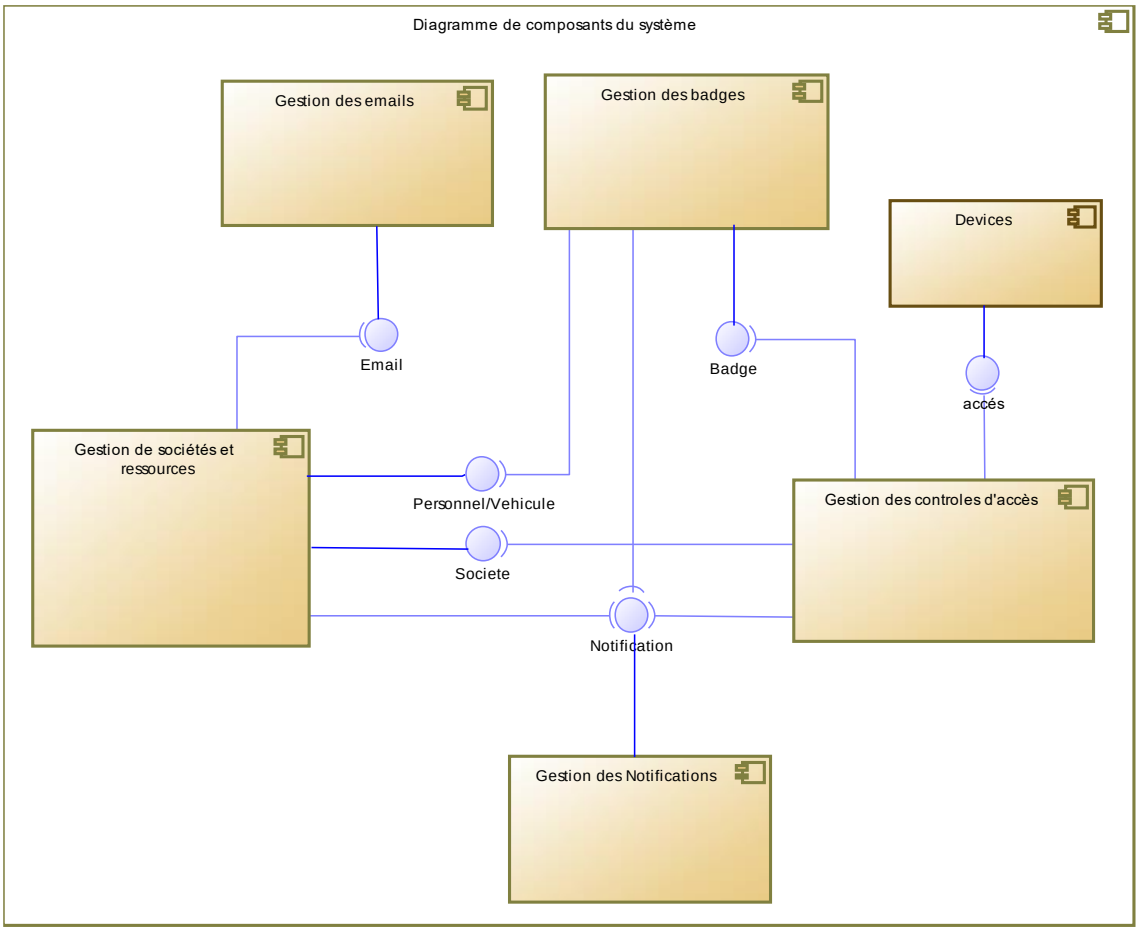


Figure 26 : Diagramme de composants

3. Diagramme de paquetage

Ce diagramme propose une vue détaillée de l'organisation et du regroupement des composants logiciels, offrant ainsi une compréhension approfondie de l'architecture logicielle et de ses interactions. Il simplifie la gestion des dépendances entre les modules et permet une visualisation claire de la structure globale du système. En fournissant une représentation visuelle, il facilite également la communication et la collaboration entre les membres de l'équipe travaillant sur le projet.

Les **figures 27, 28 et 29** montrent respectivement les diagrammes de paquetage des microservices de gestions des sociétés et des ressources, de gestion des contrôles d'accès et de la gestion des badges et profils d'accès.

❖ Diagramme de paquetage du microservice de gestion des sociétés et des ressources

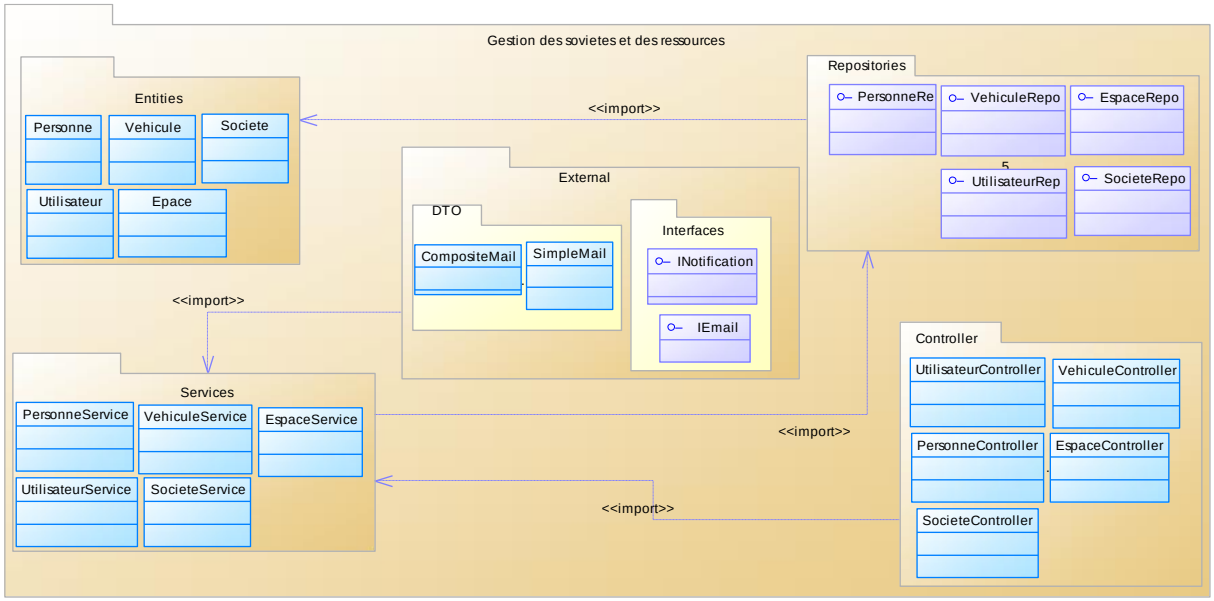


Figure 27 : Diagramme de paquetage pour le microservice de gestion des sociétés et des ressources

❖ Diagramme de paquetage du microservice de gestion des contrôles d'accès

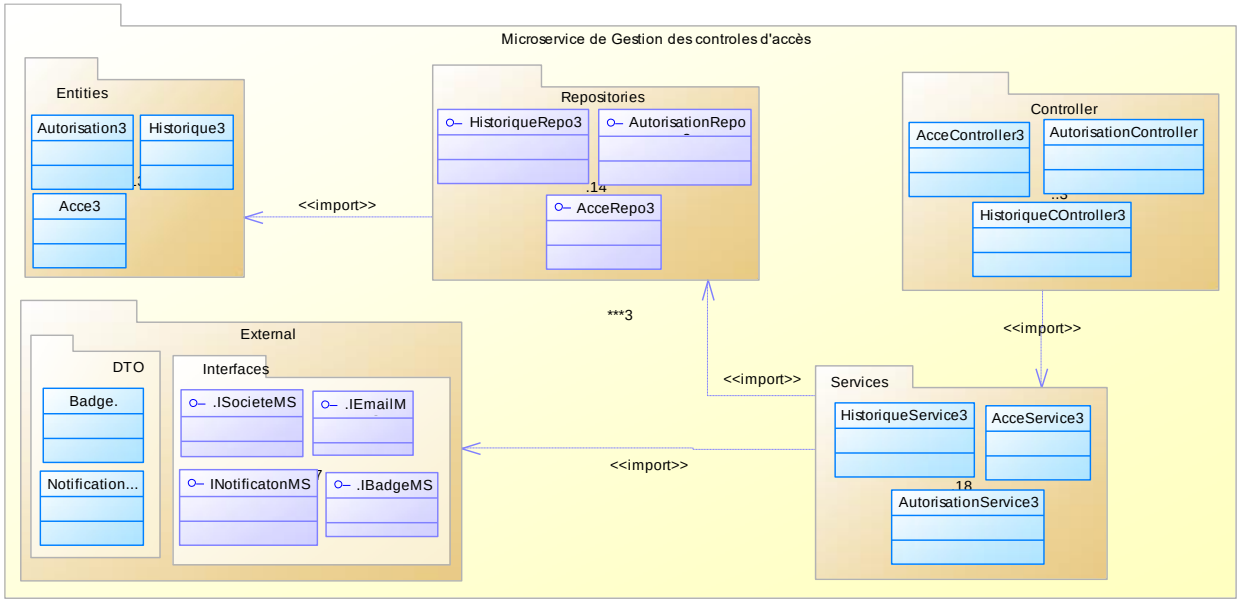


Figure 28 : Diagramme de paquetage pour le microservice de la gestion des contrôles d'accès

❖ Diagramme de paquetage du microservice de gestion des badges et profils d'accès

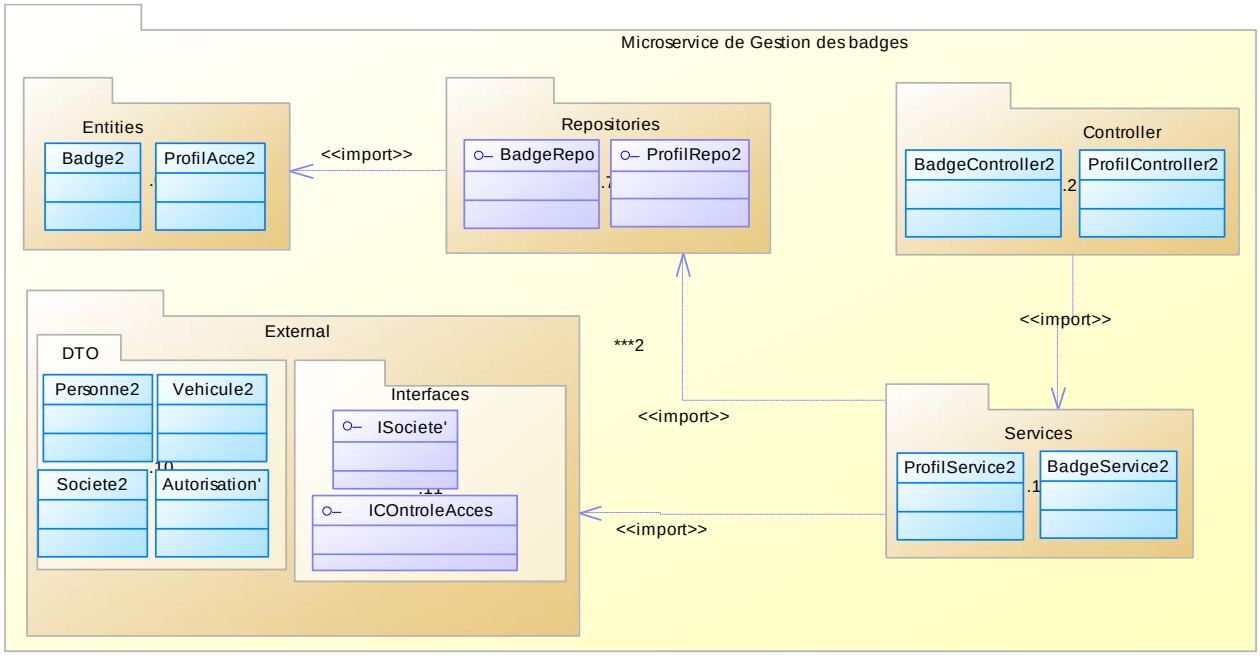


Figure 29 : Diagramme de paquetage pour le microservice de la gestion des badges et profils d'accès

4. Diagramme de déploiement

Ce diagramme offre une représentation visuelle de la répartition des composants logiciels sur le matériel physique, dévoilant la topologie du système. Il procure une compréhension approfondie des interactions entre les divers éléments matériels, essentielles pour soutenir le bon fonctionnement du logiciel. En outre, il simplifie la gestion des configurations matérielles du système en fournissant une vision claire de la manière dont les composants interagissent et sont déployés sur le plan physique.

La **figure 30** montre le diagramme de déploiement du système.

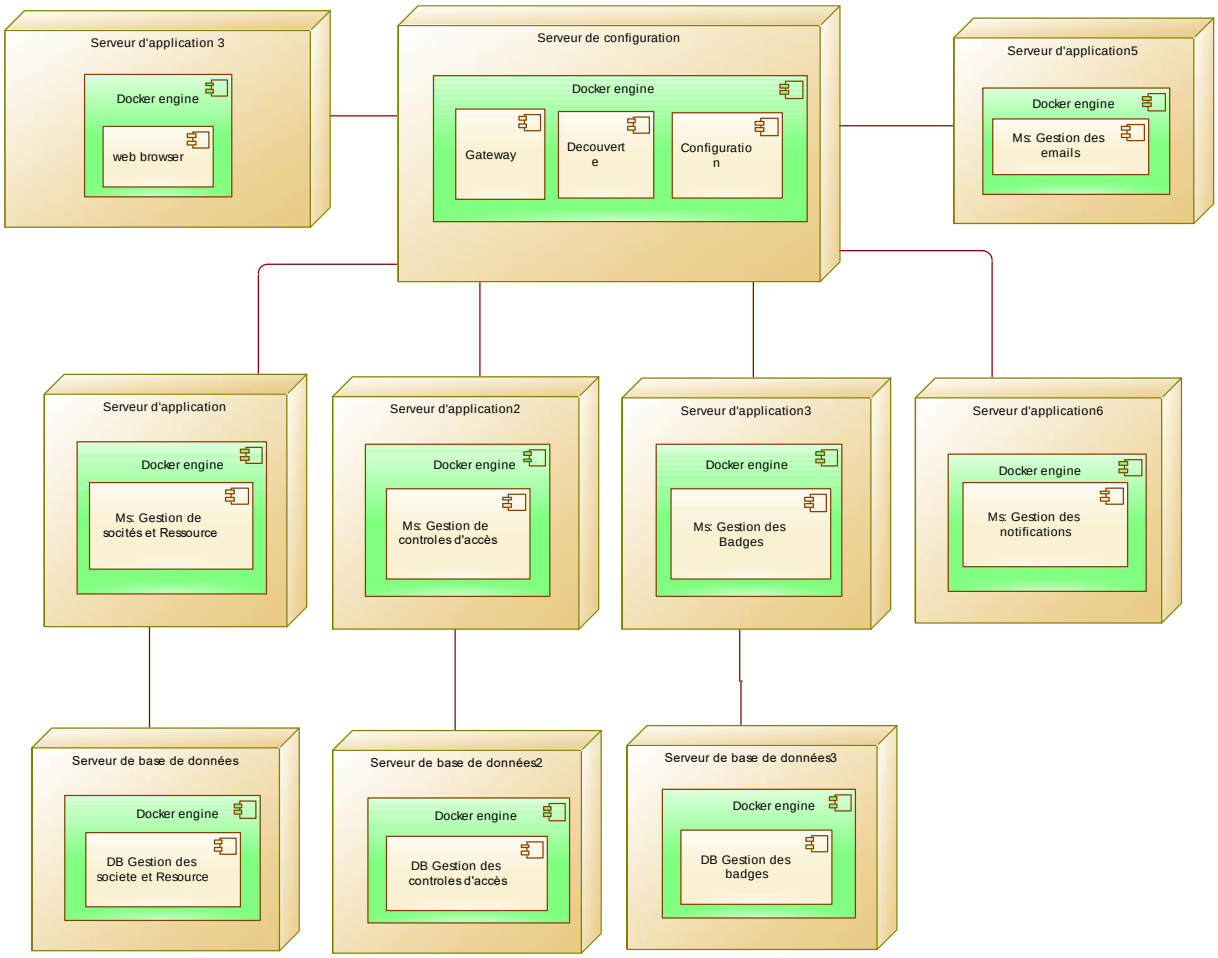


Figure 30 : Diagramme de déploiement du système

II. Conception détaillée du système

1. Diagrammes de classe

Ce diagramme offre une modélisation des entités du système et de leurs interrelations, fournissant ainsi une représentation visuelle des données et de la logique sous-jacente du programme. Il simplifie la phase de conception, facilite la documentation et améliore la compréhension de l'architecture logicielle, offrant une vue transparente des liens et des interactions entre les divers composants du système.

- ❖ Diagramme de classe de la gestion des sociétés et des ressources

La **figure 31** montre le diagramme de classe du microservice de la gestion des sociétés et de leurs ressources.

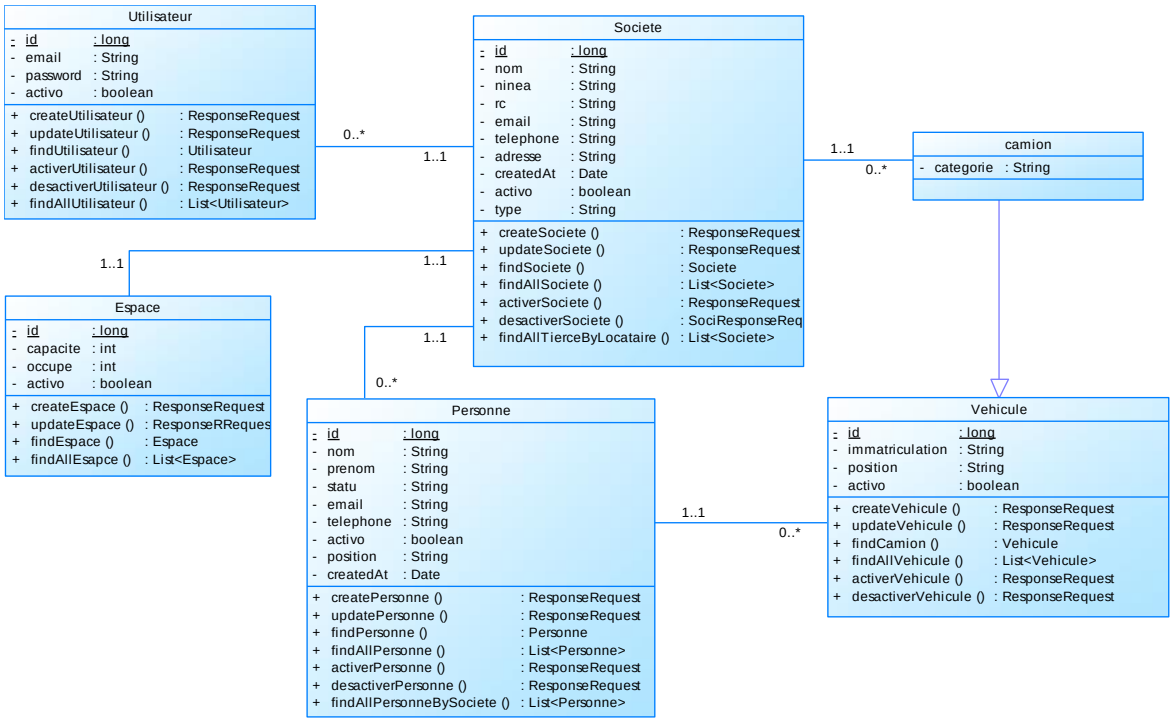


Figure 31 : Diagramme de classe de la gestion des sociétés et de leurs ressources

❖ Diagramme de classe de la gestion des badges et profils d'accès

La **figure 32** montre le diagramme de classe du microservice de la gestion des badges et des profils d'accès.

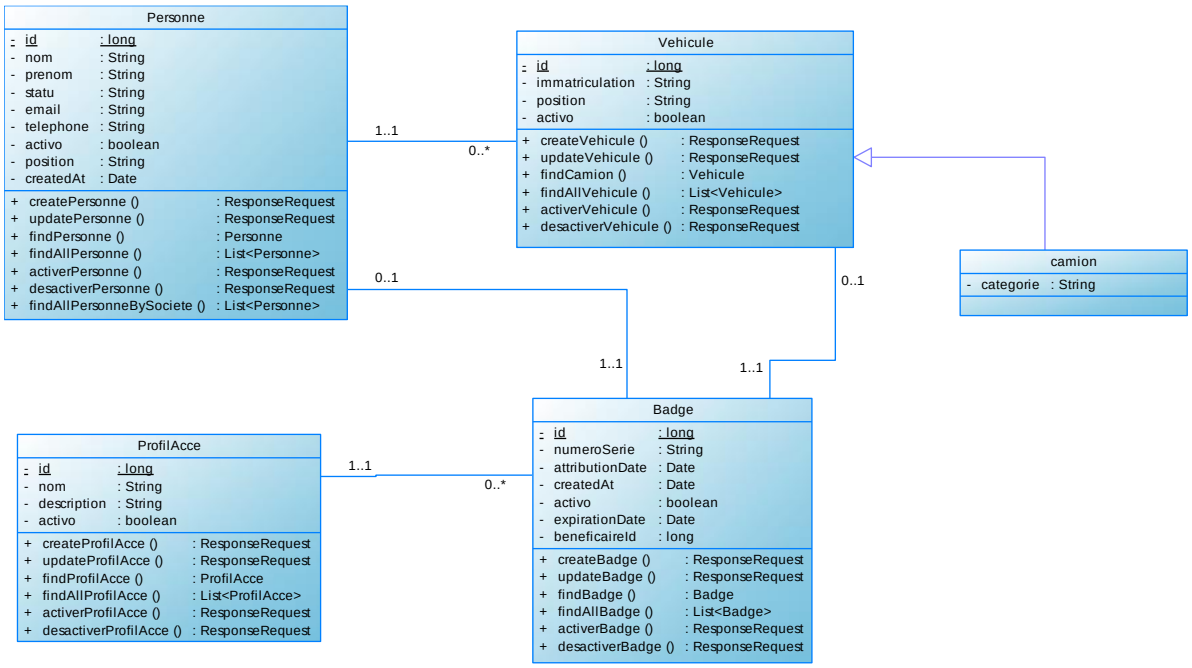


Figure 32 : Diagramme de classe de la gestion des badges et des profils d'accès

❖ Diagramme de classe de la gestion du contrôle d'accès

La **figure 33** montre le diagramme de classe du microservice de la gestion du contrôle d'accès.

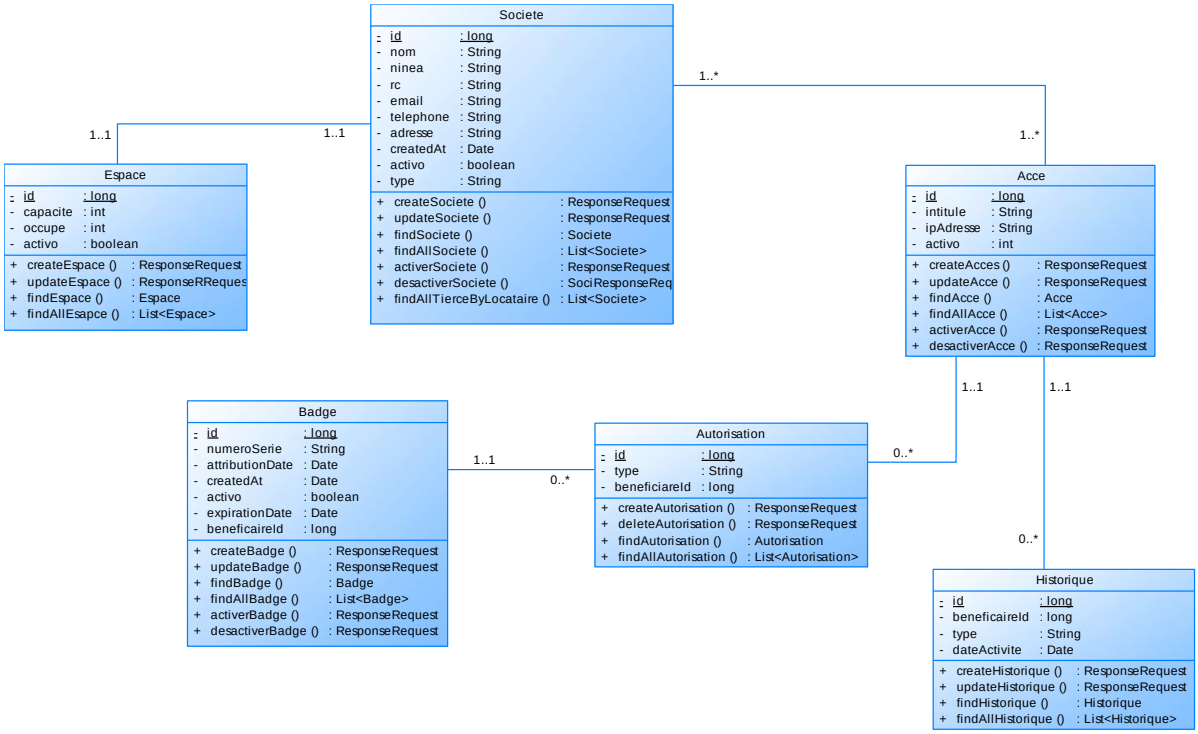


Figure 33 : Diagramme de classe de la gestion du contrôle d'accès

2. Dictionnaire de données

Le dictionnaire des données, véritable pilier de notre système d'information, constitue le recueil exhaustif et organisé de toutes les informations essentielles à notre compréhension et à notre gestion des données.

Classes	Attributs	Description	Type
Societe	id	identifiant de la société	Long
	nom	nom de la société	String
	registreCommerce	registre de commerce de la société	String
	ninea	NINEA de la société	String
	email	adresse email de la société	String
	telephone	numéro de téléphone de la société	String
	activo	etat de la société (actif ou inactif)	Boolean
Personne	id	identifiant de la personne	Long
	nom	nom de la personne	String
	prenom	prénom de la personne	String
	email	adresse email de la société	String
	telephone	numéro de téléphone de la personne	String
	position	position actuelle (intérieur ou extérieur)	String
	activo	etat de la personne (actif ou inactif)	Boolean
Utilisateur	id	identifiant de l'utilisateur	Long
	email	adresse email de l'utilisateur	String
	password	mot de passe de l'utilisateur	String
	activo	etat de l'utilisateur (actif ou inactif)	Boolean
Acces	id	identifiant de l'accès	Long
	nom	nom de l'accès	String
	ipAdresse	adresse IP de l'accès	String
	activo	etat de l'accès (actif ou inactif)	
Camion	id	identifiant de la voiture	Long
	immatriculation	immatriculation du camion	String
	categorie	catégorie du camion	String
	position	position actuelle	String
	activo	etat du camion (actif ou inactif)	Boolean

Classes	Attributs	Description	Type
Badge	id numeroSerie dateExpiraiton activo	identifiant du badge numéro de série du badge date d'expiration du badge état du badge (actif ou inactif)	Long String Date Boolean
Autorisation	id type	identifiant de l'autorisation type d'autorisation (Entrée ou sortie)	Long String
Profil	id nom description activo	identifiant du profil d'accès nom du profil d'accès description du profil d'accès état du profil (actif ou inactif)	Long String String Boolean
Role	id nom	identifiant du rôle de connexion nom du rôle de connexion	Long String
Historique	id date type	identifiant de l'historique date de l'activité (Entrée ou sortie) type de l'activité(Entrée ou sotie)	Long Date String
Espace	id capacite occupe	identifiant de l'espace capacité d'accueil de camions octroyé a une société locataire capacité occupée de camions d'une société locataire	Long Integer Integer

Tableau 11 : Dictionnaire de données

Conclusion

La démarche engagée dans la conception de système de contrôle d'accès s'inscrit dans une volonté résolue de créer une solution parfaitement adaptée à nos besoins. Ce chapitre éclaire notre chemin vers la réalisation d'un système, soulignant la souplesse et la précision inhérentes à notre approche.

Chapitre 6 : Implémentation, simulation et présentation du système

Introduction

L'implémentation, la simulation et la présentation d'un système jouent un rôle central dans le cycle de vie du développement logiciel, façonnant la concrétisation des idées théoriques en solutions pratiques. Ce chapitre explore le processus d'implémentation du système de contrôle d'accès spécifique, les choix de technologies et la présentation de l'API mise en place, des interfaces utilisateurs et une simulation sur ordinateur et une simulation physique avec des composants arduino offrant une vue claire du système développé.

I. Implémentation du système

1. Outils et technologies

L'implémentation du système de contrôle d'accès a été réalisée en utilisant plusieurs outils et langages de développement afin d'assurer une expérience de développement efficace et collaborative. Les principaux outils et langages utilisés sont représentés respectivement dans les **tableaux 12 et 13**.

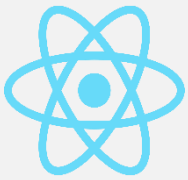
❖ **Outils**

Outils	Description	Version	Logos
Visual Studio Code	Choisi pour son interface légère, ses nombreuses extensions, et son support intégré pour les technologies web	1.84.2	
IntelliJ	Utilisé en tant qu'environnement de développement intégré (IDE) offrant des fonctionnalités avancées pour le développement Java	2023.1	
Postman	Employé pour tester les API et les services, permettant une validation rapide des fonctionnalités développées.	10.21.0	

Outils	Description	Version	Logos
Github	Utilisé pour le stockage de code source collaboratif, le partage et la collaboration sur des projets de développement.		
Git	Adopté pour le suivi efficace des changements dans le code source et une collaboration transparente entre les membres de l'équipe de développement.	2.40.0	
Expo	Utilisé pour permettre aux développeurs d'écrire des applications mobiles en utilisant JavaScript et React Native	50.0.8	
Docker	plateforme de conteneurisation qui permet d'encapsuler des applications et leurs dépendances dans des conteneurs légers et portables	4.20.0	
Grafana	Utilisé pour visualiser et analyser les métriques collectées par les systèmes de surveillance.	10.3.3	
Prometheus	Utilisé pour collecter des métriques à partir de cibles configurées à des intervalles spécifiés, les stocke et les rend disponibles pour des requêtes et des alertes.	2.50	
Zipkin	Utilisé pour suivre et de visualiser le flux des requêtes à mesure qu'elles passent à travers différents services	3.1	
SpringDoc OpenAPI	bibliothèque qui permet de générer automatiquement une documentation OpenAPI (anciennement Swagger) pour les API REST	2.3.0	

Tableau 12 : Outils utilisés

❖ **Technologies**

Outils	Description	Version	Logos
HTML (HyperText Markup Language	Utilisé pour la structure de la page web.	5	
CSS (Cascading Style Sheets)	Employé pour le stylisme et la mise en page des éléments HTML.	3	
TypeScript (TS)	Choisi pour le développement côté client, permettant une programmation et une maintenance facilitée.	4.6.4	
Angular	Utilisé comme framework front-end, fournissant une structure robuste et des fonctionnalités avancées pour le développement d'applications web dynamiques.	16.0.0	
React Native	framework pour créer des applications mobiles multiplateformes en utilisant le langage de programmation JavaScript et la bibliothèque React.	0.73.4	
Java	Utilisé pour offrir une base solide et des fonctionnalités avancées pour la création d'applications web dynamiques grâce à des frameworks bien établis tels que Spring.	17.3.0.1	
Spring Boot	Choisi comme framework pour le développement d'applications Java, offrant une configuration simplifiée et des fonctionnalités prêtes à être utilisées.	3.2.1	

Outils	Description	Version	Logos
Spring Security	Intégré pour la gestion des aspects liés à la sécurité de l'application, y compris l'authentification et l'autorisation.	6	
JSON Web Token (JWT)	Utilisé comme mécanisme d'authentification sécurisé pour les communications entre les composants du systèmes		
Spring Data JPA	Employé pour la gestion simplifiée des interactions avec la base de données PostgreSQL	3.2.1	
PostegreSql	choisi pour stocker et gérer les données de manière efficace, assurant la cohérence et l'intégrité des informations au sein du système.	11	
Spring Cloud	Utilisé pour faciliter le développement, le déploiement et la gestion d'applications distribuées basées sur des microservices dans des environnements cloud.	2022.0.4	

Tableau 13 : Technologies utilisées

II. Simulation

Une attention particulière a été portée à la simulation, permettant ainsi une approche pratique et informatique pour évaluer le système de contrôle d'accès proposé. Pour ce faire, deux méthodes de simulation ont été employées : une simulation physique réalisée à l'aide de montages Arduino pour reproduire le fonctionnement de l'entrée principale, ainsi qu'une simulation sur ordinateur.

1. Simulation sur ordinateur

Nous avons réalisé une simulation sur ordinateur permettant de matérialiser les différentes zones d'accès par des compartiments, chacun étant représenté par un trait bleu symbolisant une barrière virtuelle.

La **figure 34** montre la représentation virtuelle des zones et entrées distingués au sein de la plateforme de distribution.

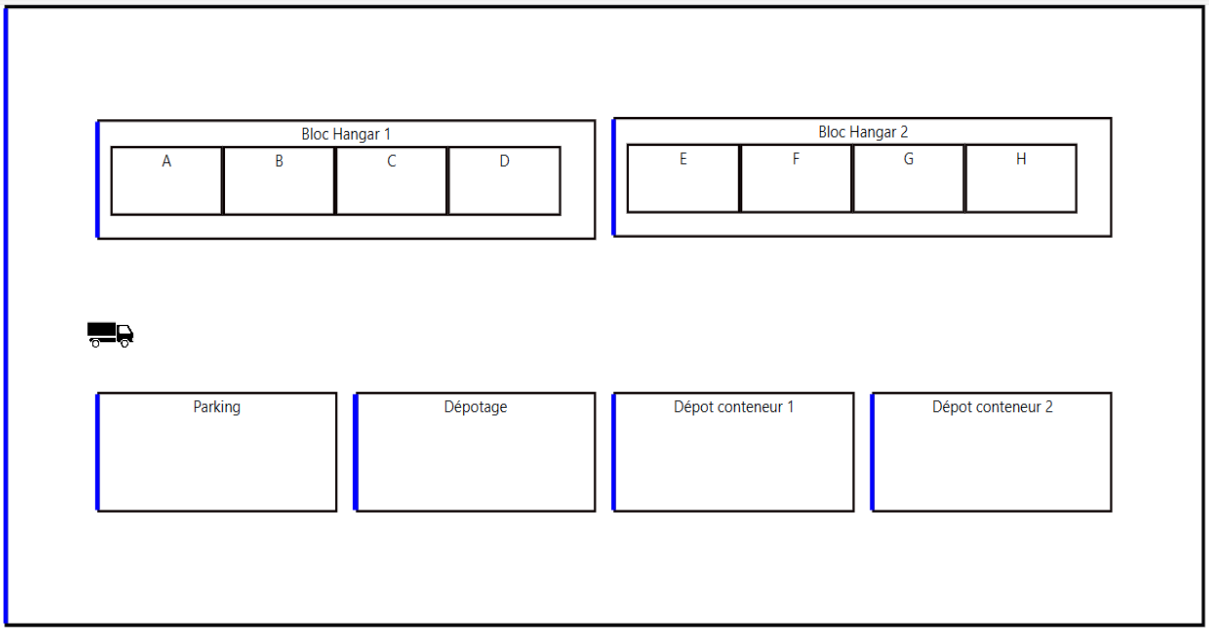


Figure 34 : Représentation virtuelle des entrées de la plateforme

Lorsqu'un badge d'accès est présenté au lecteur, le système effectue une vérification de l'autorisation associée à ce badge. Si l'accès est autorisé, le trait bleu se transforme en vert et effectue une rotation pour indiquer un accès valide comme le montre la **figure 35**.

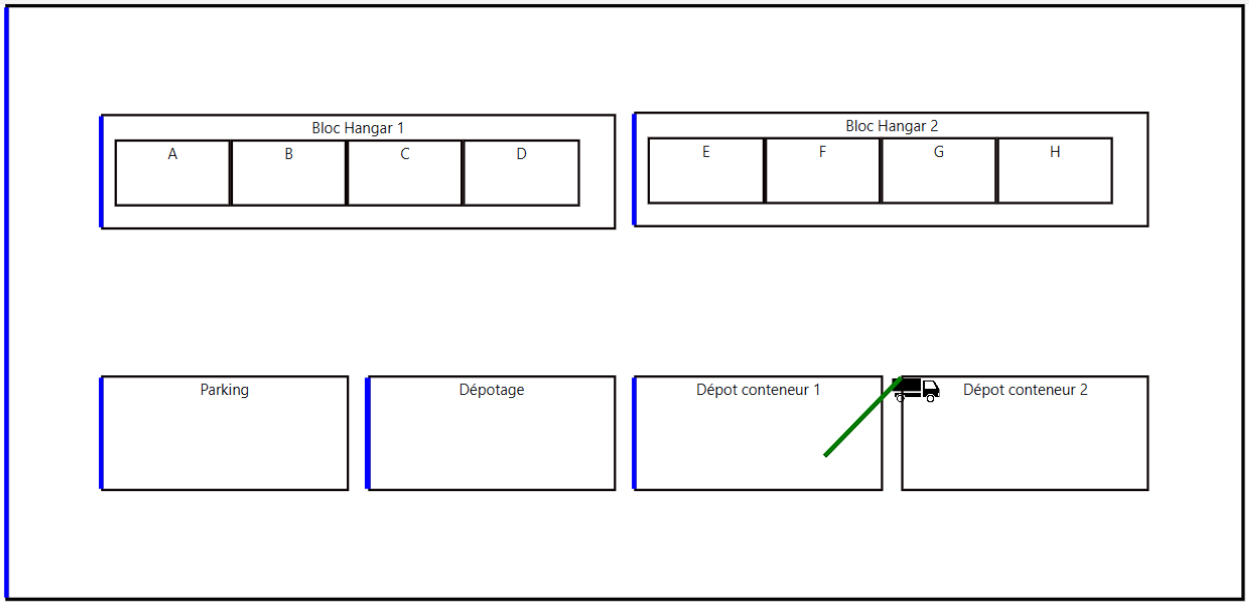


Figure 35 : Représentation d'une entrée valide

En revanche, si l'accès est refusé, le trait bleu devient rouge pour signaler un accès non autorisé comme le montre la **figure 36.**

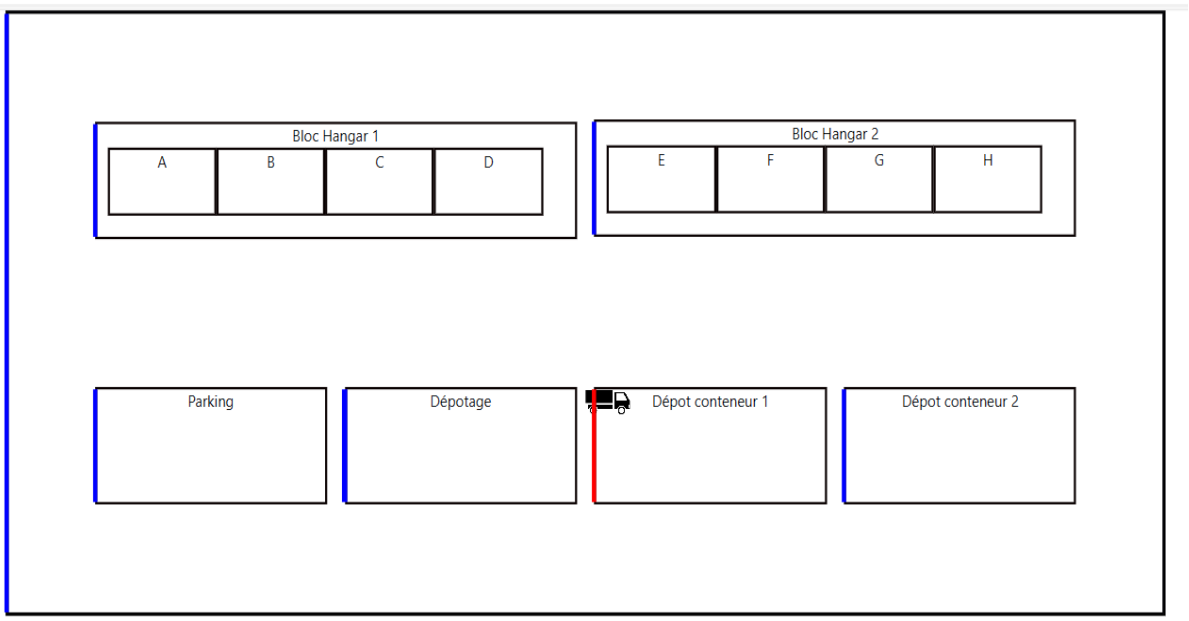


Figure 36 : Représentation d'une entrée non valide

Cette simulation permet de visualiser de manière interactive le fonctionnement du système de contrôle d'accès, offrant ainsi une compréhension visuelle et pratique de son mécanisme de fonctionnement.

2. Simulation physique

Dans cette section, nous avons réalisé deux montages distincts, chacun servant à des fonctions spécifiques au sein du système. Le premier montage est dédié à l'enregistrement et à l'octroi de badges, tandis que le second est dédié au contrôle d'accès.

❖ Outils et Technologies utilisés

Nom	Rôles	Images
Arduino IDE	Environnement de développement intégré (IDE) spécialement conçu pour la programmation des microcontrôleurs Arduino.	
Circuit.io	Plateforme en ligne pour la conception et la simulation de circuits électroniques. Permet de modéliser visuellement les connexions entre les composants avant leur implémentation physique.	

Nom	Rôles	Images
Langage C	Langage de programmation utilisé dans le développement de logiciels pour Arduino. Le code écrit en langage C est interprété et exécuté par le microcontrôleur Arduino pour contrôler le fonctionnement des montages électroniques.	

Tableau 14 : Outils et technologies pour le système de contrôle d'accès

❖ Montage 1 : Enregistrement et Octroi de Badge

Dans cette première étape du projet, nous avons déployé un montage avec l'Arduino Mega 2560 comme unité centrale, un mini breadboard pour faciliter les connexions et un lecteur de badge RFID pour lire les informations des cartes ou des tags.

Le processus débute par la détection d'une carte à l'aide du lecteur RFID. Le numéro de série de la carte ou du tag est ensuite extrait par le lecteur RFID.

Les informations, y compris le numéro de série, sont transférées au formulaire d'enregistrement et d'attribution par l'Arduino Mega 2560.

La **figure 37** montre le processus et les composants utilisés pour réaliser le montage qui permet l'enregistrement et l'octroi de badge.

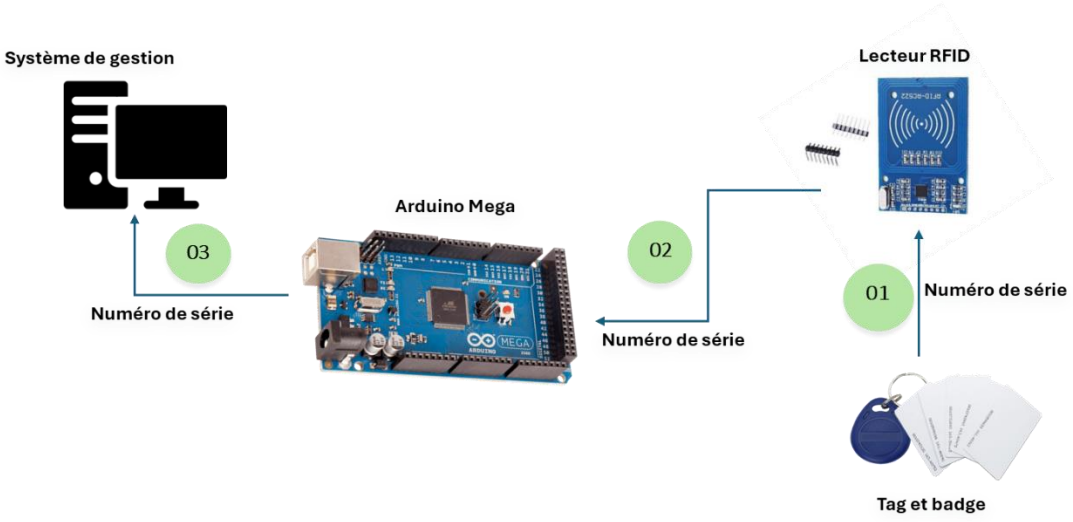


Figure 37 : Processus de récupération d'identifiant de badge pour son attribution

La **figure 38** montre le circuit physique correspondant au montage Arduino pour la récupération de numéro de série des badges RFID

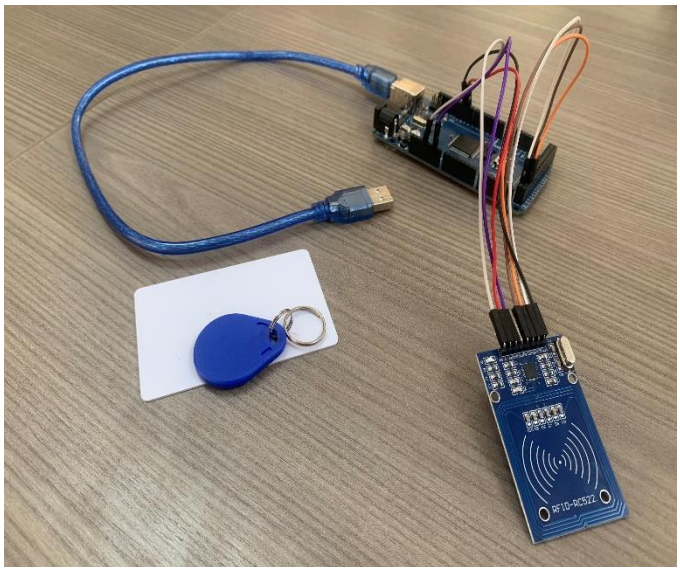


Figure 38 : Montage pour le circuit de récupération de numéro série des badges

❖ **Montage 2 : Contrôle d'Accès**

Dans ce montage, le lecteur de badge RFID reste en permanence à l'écoute. Lorsqu'un badge est détecté, son numéro de série est envoyé au backend pour vérifier s'il est autorisé à accéder à la plateforme. Si l'accès est autorisé, le servomoteur soulève la barrière jusqu'à ce que le capteur ultrasonique ne détecte plus de présence, indiquant ainsi que le véhicule est passé. Ensuite, la barrière se referme, prête pour le prochain accès.

La **figure 39** montre le processus et les composants utilisés pour réaliser le montage qui permet de contrôler l'accès.

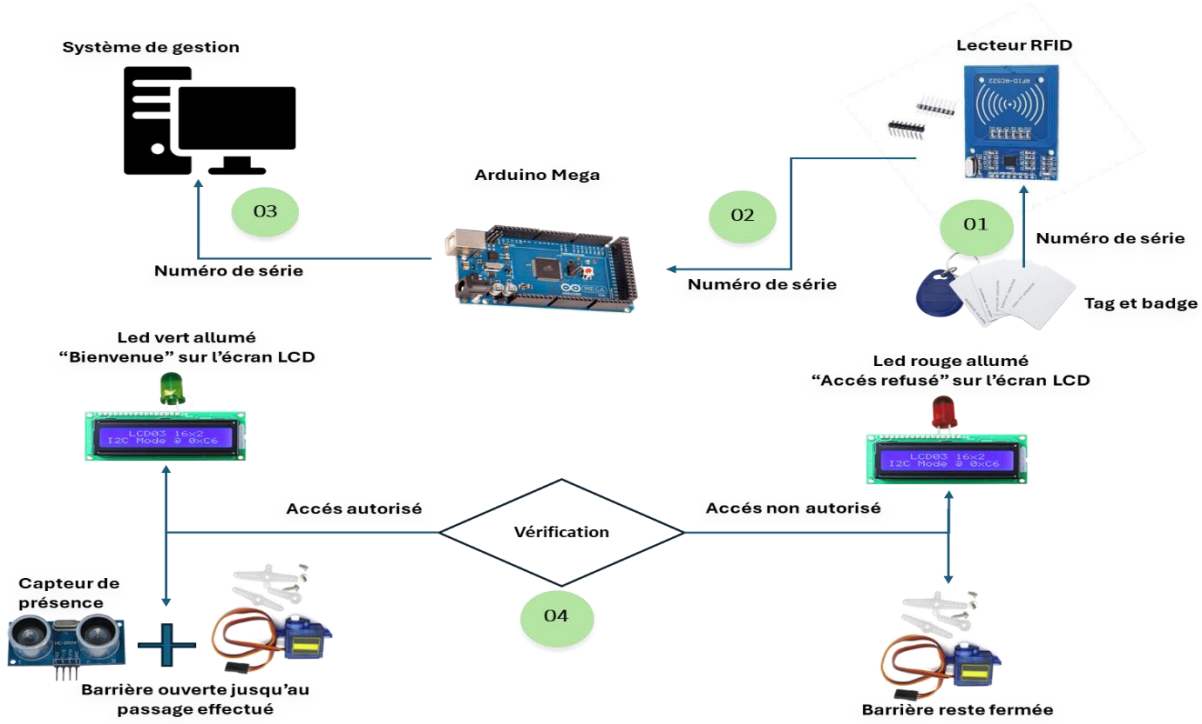


Figure 39 : Processus et composants pour le contrôle d'accès

La **figure 40** montre le circuit physique correspondant au montage Arduino pour le contrôle d'accès.

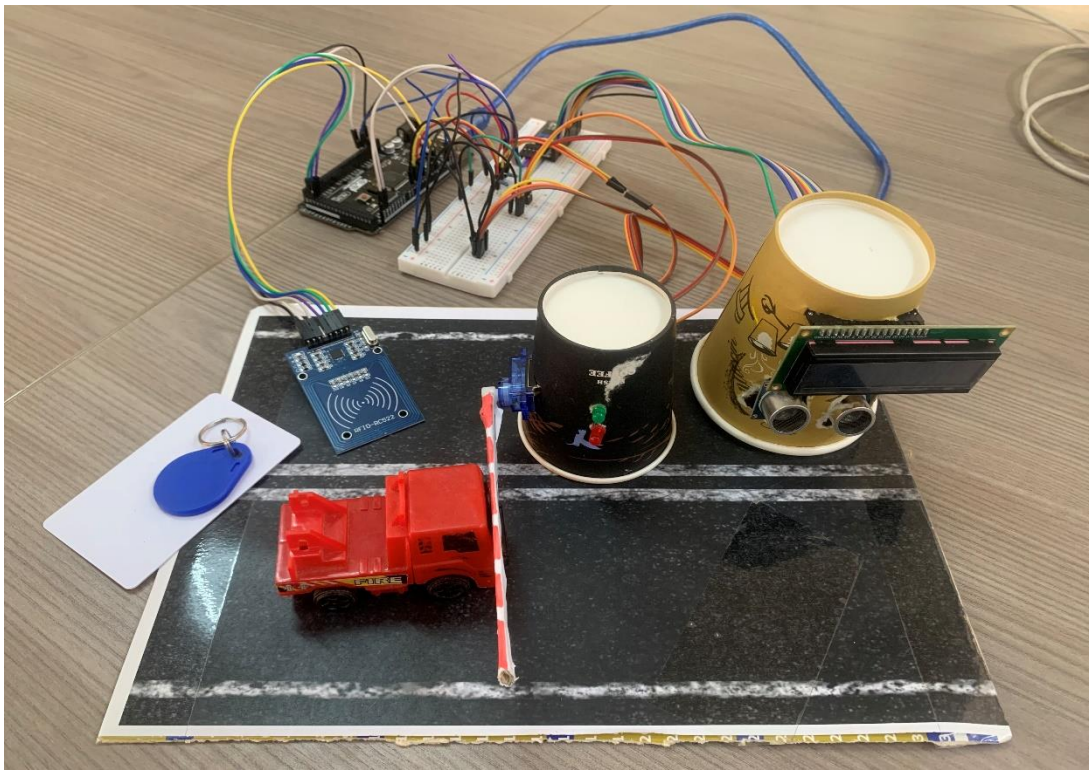


Figure 40: Montage pour le circuit de contrôle d'accès

III. Présentation du système

Au cours des différentes étapes d'analyse et de conception que nous avons traversées, nous avons réussi à élaborer un système dédié au contrôle d'accès sur la plateforme. Ce système répond aux exigences, permettant la gestion numérique de l'accès des véhicules et des individus, tout en simplifiant le processus d'attribution des autorisation d'accès et le contrôle des accès.

1. Documentation de l'API

L'API que nous avons mise en place est conçue de manière à être indépendante et peut être utilisée et ayant les droits requis l'intégrer dans son système. Elle offre une interface standardisée pour accéder aux fonctionnalités et aux données de notre application, ce qui facilite son adoption et son utilisation par d'autres développeurs et applications.

La documentation de notre API comprend des détails sur chaque point de terminaison disponible, les méthodes HTTP supportées, les paramètres requis ou optionnels, les formats de données acceptés et renvoyés, ainsi que les éventuels mécanismes de sécurité mis en place pour protéger l'accès aux ressources.

Figure 41 : Documentation de l'API de la gestion des sociétés et de leurs ressources

Cette documentation comprend des informations sur les points de terminaisons, les paramètres acceptés, les réponses renvoyées, les exemples d'utilisation comme le montre **les figures 42, 43** et **44** .

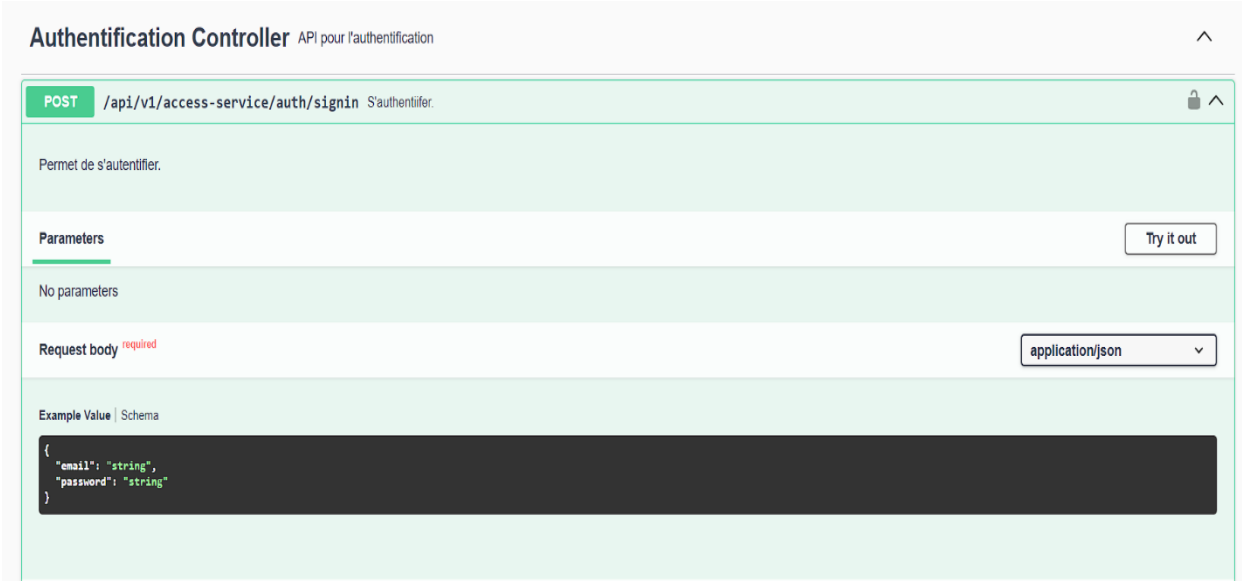


Figure 42 : Paramètres et corps de la requête pour l'authentification

Figure 43 : Descriptif de la réponse de la requête de l'authentification

Pour pouvoir accéder à certaines fonctionnalités un token est requis comme le montre la **figure 29** :

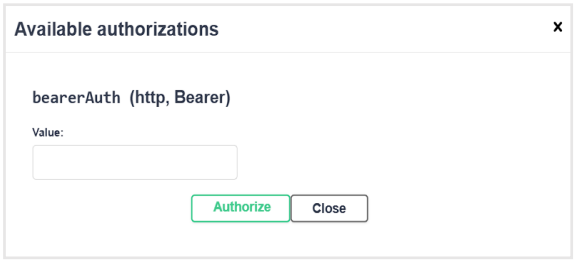


Figure 44 : Sécurisation des endpoints

En fournissant une documentation complète et claire, nous visons à rendre l'intégration de notre API aussi fluide que possible pour les développeurs tiers, tout en garantissant la sécurité et la fiabilité des interactions avec notre système.

2. Présentation des interfaces web et mobiles

Dans cette partie, nous illustrerons des interfaces utilisateur web et mobiles développées, offrant une expérience conviviale et intuitive pour les utilisateurs.

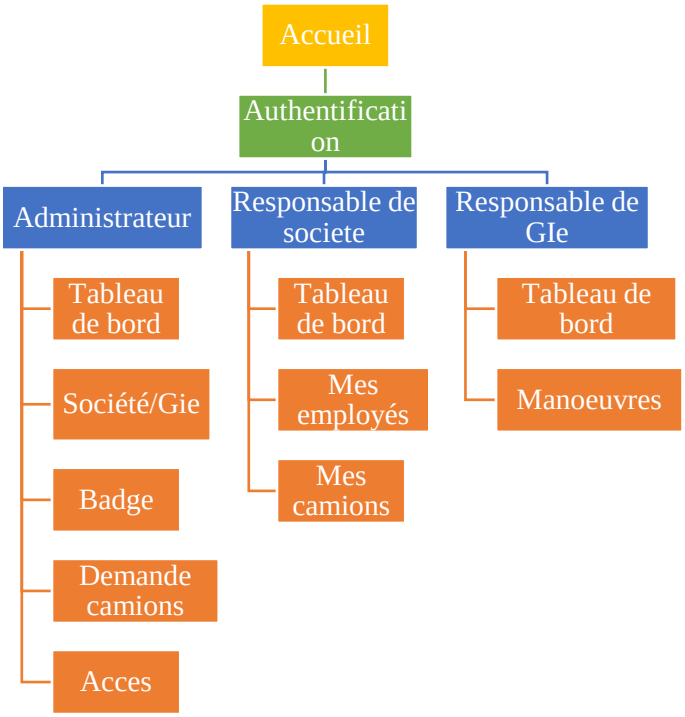


Figure 45 Vue globale du système

a. Authentification

Ces interfaces permettent à différents utilisateurs de se connecter. Une fois que l'utilisateur fournit un identifiant et un mot de passe corrects, il est dirigé vers son tableau de bord.

❖ **Web** **Mobile**

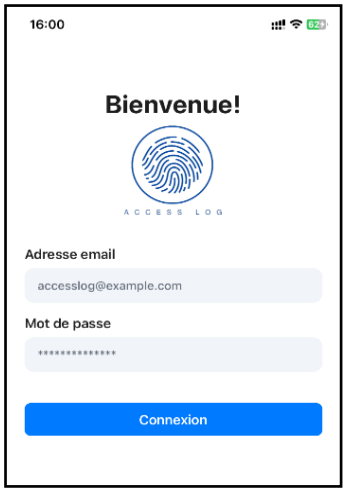


Figure 47 : Page web d'authentification *Figure 46 : Page mobile d'authentification*

b. Administrateur

Après une authentification réussie, l'administrateur peut accéder à une vue globale de la plateforme comme le montre la **figure 48**.

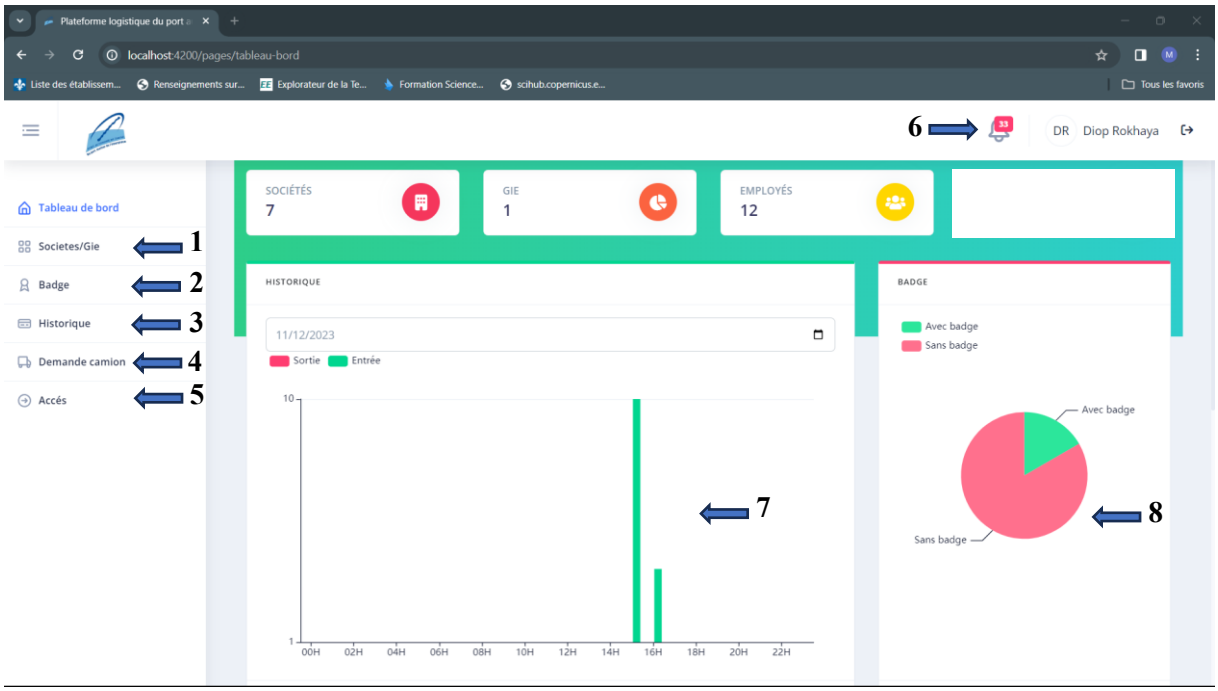


Figure 48 Tableau de bord de l'administrateur

- **1** : mène vers l'interface les sociétés locataires et GIE qui sont dans la plateforme de distribution

- **2** : mène vers l'interface qui gère les demandes des badges des employés des sociétés locataires et les manœuvres des GIE.
- **3** : mène vers l'interface qui affiche l'ensemble des historiques d'entrée et de sortie.
- **4** : mène vers l'interface qui gère les demandes des badges des camions des sociétés locataires
- **5** : mène vers l'interface qui gère les accès.
- **6** : permet d'afficher le ruban des dernières notifications
- **7** : visualise le nombre d'entrée et de sortie par heure pour une journée donnée
- **8** : visualise le nombre de camions et de personnes ayant un badge (vert) et non (vert) suite à une demande.

❖ **Mobile**

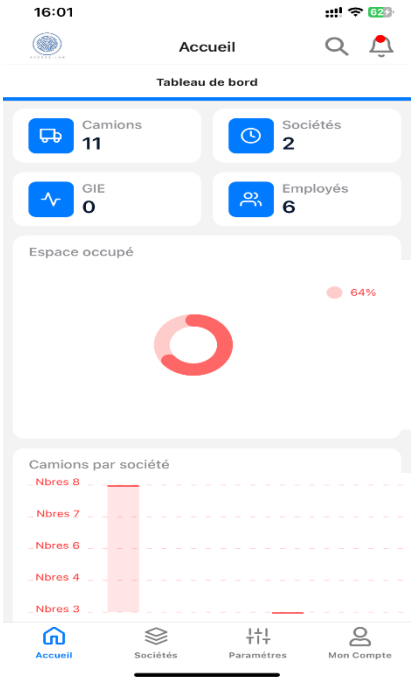


Figure 49 : Tableau de bord mobile de l'administrateur

Il est chargé de gérer l'attribution des cartes d'accès aux employés et aux camions, avec la possibilité de déterminer le profil auquel la carte doit appartenir (mensuel, trimestriel, semestriel, annuel etc.) .

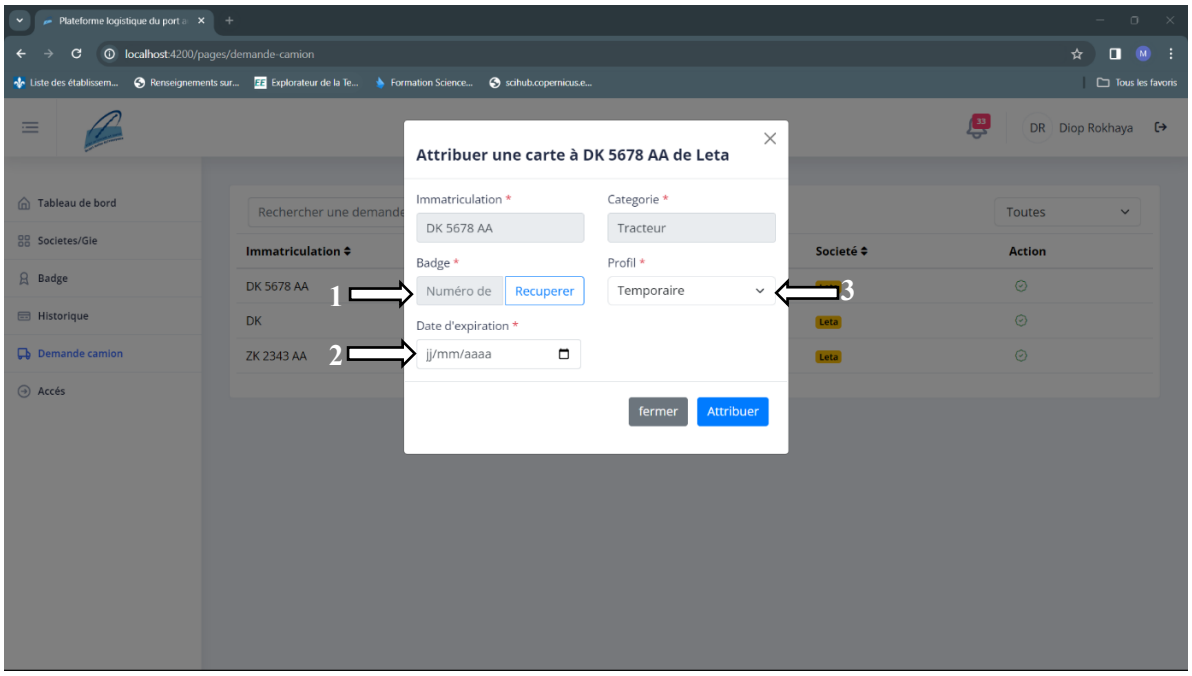


Figure 50 : Attribuer badge à un camion

- **1 :** récupère le numéro de série du badge posé sur le lecteur RFID.
- **2 :** définit la date à laquelle le badge ne devient plus actif
- **3 :** permet de définir le profil auquel le badge doit appartenir

L'administrateur reçoit en temps réel des informations, notamment les demandes de cartes et les entrées/sorties de la plateforme.

c. Responsable de société

Suite à une authentification réussie, le responsable de chaque société peut accéder à son tableau de bord, fournissant un résumé des activités de sa société lui concernant.

❖ **Web**

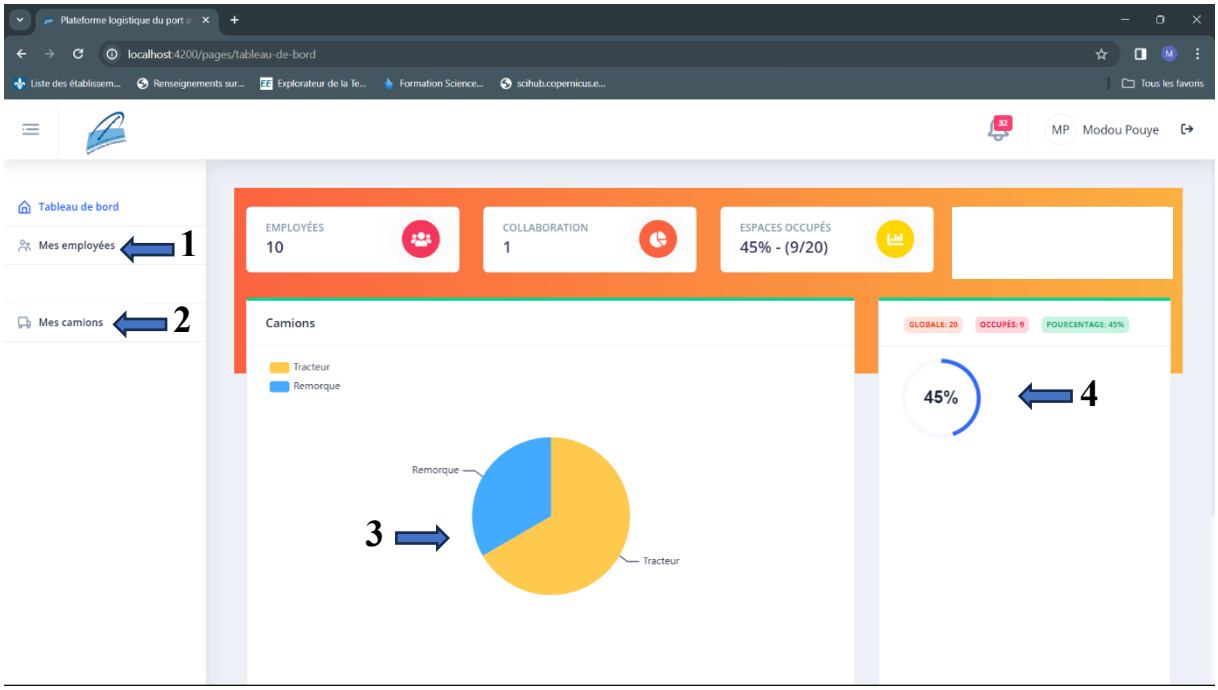


Figure 51 : Tableau de bord de Responsable de société

❖ **1 :** mène vers l'interface qui gère les employés

❖ **2 :** mène vers l'interface qui gère les camions

❖ **3 :** visualise le nombre de camion en fonction de leur catégorie

❖ **4 :** visualise le nombre de place global et occupé pour les camions alloué à la société locataire.

❖ **Mobile**

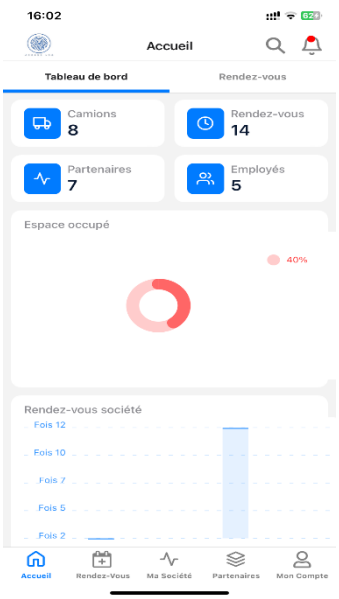


Figure 54 : Tableau de bord de l'administrateur

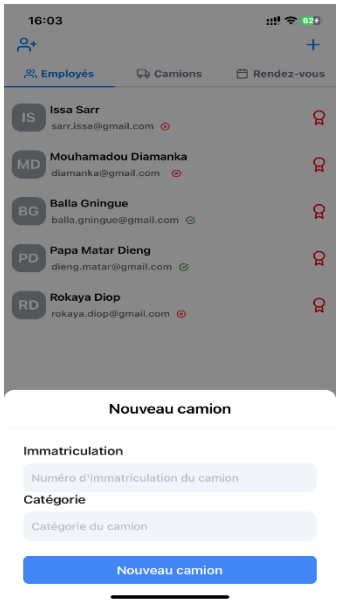


Figure 53 : Ajout de camion

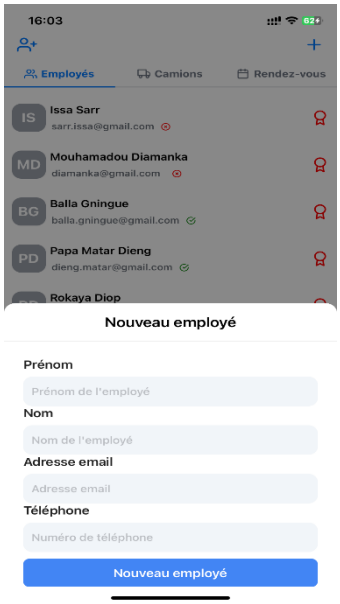


Figure 52 : Ajout d'employé

Dans l'ensemble, le système propose une gestion exhaustive tant pour l'administrateur que pour les responsables de sociétés et GIE.

Après une authentification réussie, l' administrateur peut surveiller en temps réel l'état global de la plateforme, incluant le nombre de sociétés et d'employés. De plus, il a la capacité de gérer l'attribution de cartes d'accès et de recevoir des informations en temps réel sur les demandes de cartes, les entrées et sorties de la plateforme.

Quant au responsable des société, ils peuvent visualiser le pourcentage d'occupation de l'espace, le nombre d'employés, la répartition des catégories de camions, ainsi que le statut des badges des employés. De plus, il a la possibilité de faire des demandes de badges et d'activer ou désactiver des employés.

Conclusion

En conclusion, l'implémentation, la simulation et la présentation du système ont été des phases cruciales dans le développement de cette solution. Les diverses étapes ont été abordées avec une attention particulière portée à la qualité, à la robustesse et à la conformité aux exigences fonctionnelles. En regardant vers l'avenir, ce prototypage propose également des pistes pour des améliorations continues, identifiant des domaines où des ajustements pourraient renforcer la performance, la sécurité ou la convivialité du système.

Conclusion et perspectives

Ce projet approfondi met en évidence les défis critiques auxquels la plateforme de distribution du port autonome de Dakar est actuellement confrontée en termes de sécurité et d'efficacité opérationnelle. Les lacunes identifiées dans le système de contrôle d'accès actuel ont motivé la conception d'un système visant à renforcer ces aspects vitaux.

L'analyse approfondie des lacunes, notamment les accès non autorisés et les problèmes de gestion du flux de véhicules, a souligné des risques potentiels tels que le vol, la gestion inefficace des accès, et la vulnérabilité des données sensibles.

Pour pallier à ces problématiques, nous avons réalisé un système permettant une gestion centralisée des sociétés et leurs ressources, l'attribution des autorisations d'entrée et de sortie, ainsi que le contrôle des accès. Ce système comprend le développement d'une API découplée, permettant une intégration transparente de notre système avec les applications existantes ou futures des sociétés clientes. Des interfaces utilisateur intuitives et conviviales sont également mises en place pour faciliter l'utilisation du système par les différents acteurs.

Nous avons opté pour une approche agile avec la méthodologie Scrum afin de garantir une gestion de projet efficace et flexible. Du point de vue architectural, une conception en microservices a été privilégiée pour assurer une meilleure évolutivité et une plus grande modularité du système. La technologie RFID a été retenue pour la gestion des contrôles d'accès physiques. Afin de valider notre solution, nous avons réalisé un prototype matériel utilisant des montages Arduino, ainsi qu'une simulation virtuelle complète sur ordinateur.

Cependant, concevoir un système de contrôle d'accès et un prototype physique constituent une première étape. Les perspectives futures incluent la mise en œuvre effective du système sur la plateforme de distribution du Port Autonome de Dakar, suivie d'une phase de test approfondi. Il sera essentiel de surveiller les performances du système, d'ajuster les paramètres si nécessaire, et de garantir une intégration harmonieuse avec les opérations existantes.

Concernant les perspectives futures, plusieurs axes de développement s'ouvrent :

- Utilisation de vraies barrières automatiques et de tourniquets : Passer de prototypes à des solutions matérielles complètes en adoptant l'utilisation de vraies barrières automatiques et de tourniquets. Cette évolution contribuerait à une mise en œuvre plus robuste et fiable du contrôle d'accès, offrant une réponse physique à la sécurité.

- Reconnaissance de Plaque d'Immatriculation : Envisager l'intégration d'un système de contrôle d'accès basé sur la reconnaissance de plaque d'immatriculation. Cette technologie permettrait une identification rapide et automatisée des véhicules autorisés, renforçant ainsi la sécurité et accélérant les flux de circulation.
- Amélioration de la gestion des accès piétons : Développer des solutions spécifiques pour gérer les accès des piétons, en intégrant des systèmes de reconnaissance faciale pour un contrôle d'accès plus sécurisé et fluide.

Ces perspectives reflètent une vision holistique pour l'optimisation continue du contrôle d'accès sur la plateforme de distribution. La mise en œuvre de ces avancées technologiques offrira une solution complète, répondant aux exigences croissantes de sécurité et d'efficacité opérationnelle, et positionnera la plateforme en tant que référence dans le domaine du commerce international

Annexes

Annexe 1 : Lancement des outils de supervision sur docker

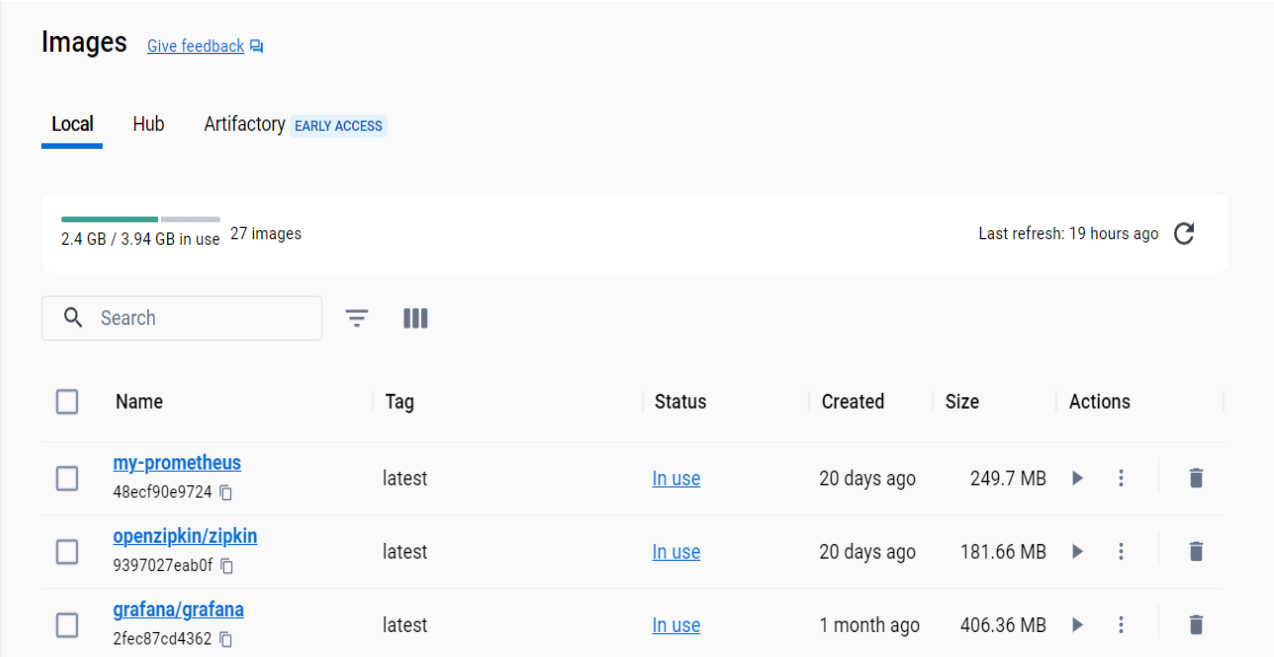


Figure 55 : Lancement des outils de supervision avec docker

Annexe 2 : Tableau de bord de Grafana

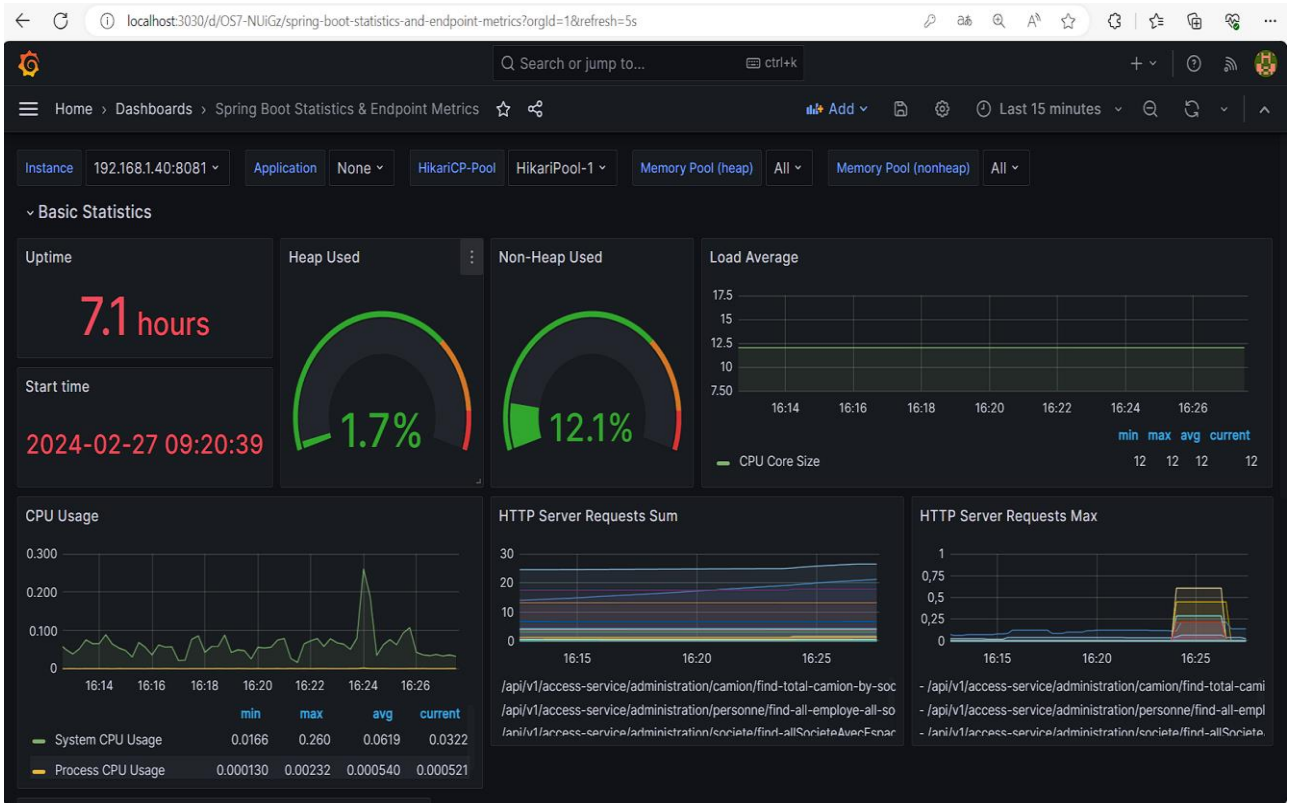


Figure 56 : Tableau de bord de Grafana

Annexe 3 : Tableau de bord de Spring boot Admin

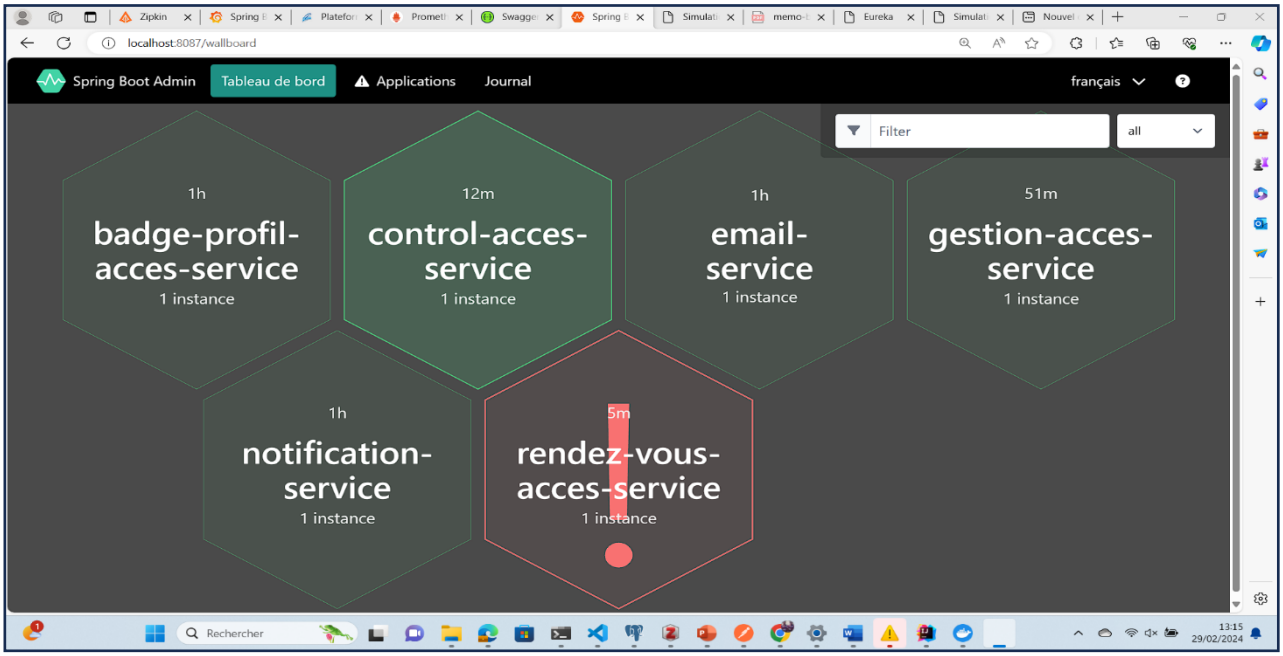


Figure 57 : Tableau de bord Spring boot admin

Annexe 4 : Tableau d'instances de Prometheus

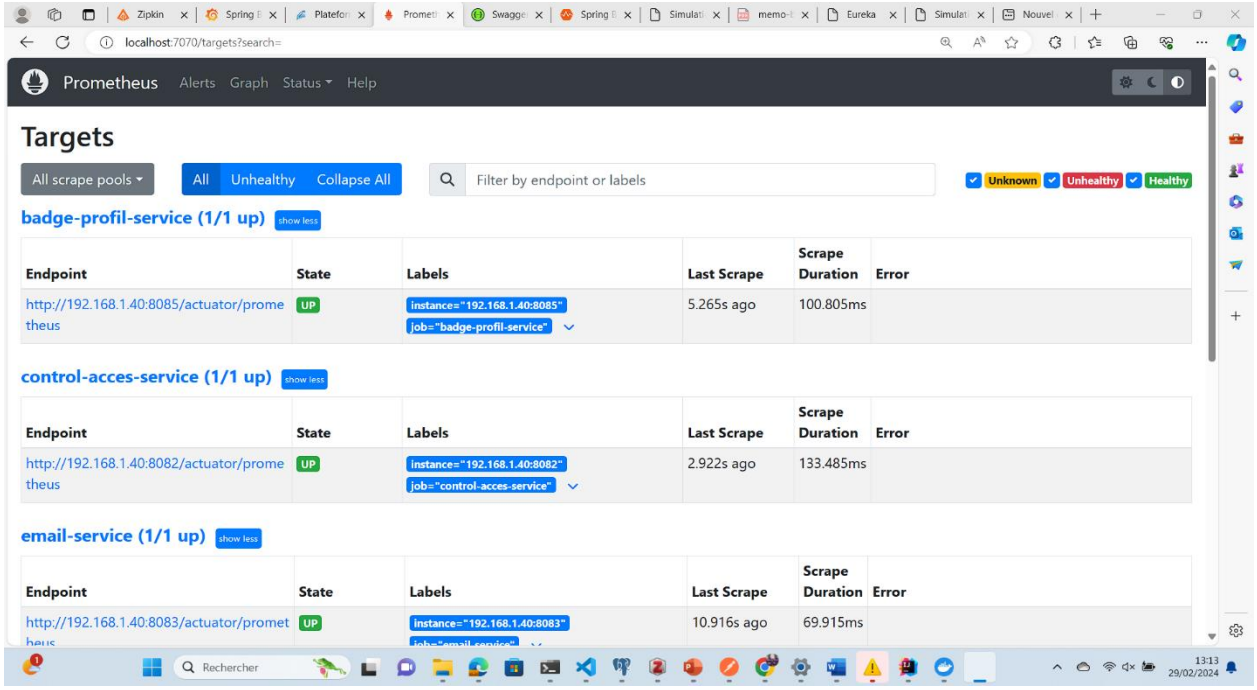


Figure 58 : Tableau de bord de Prometheus

Annexe 5 : Suivi des requête avec Zipkin

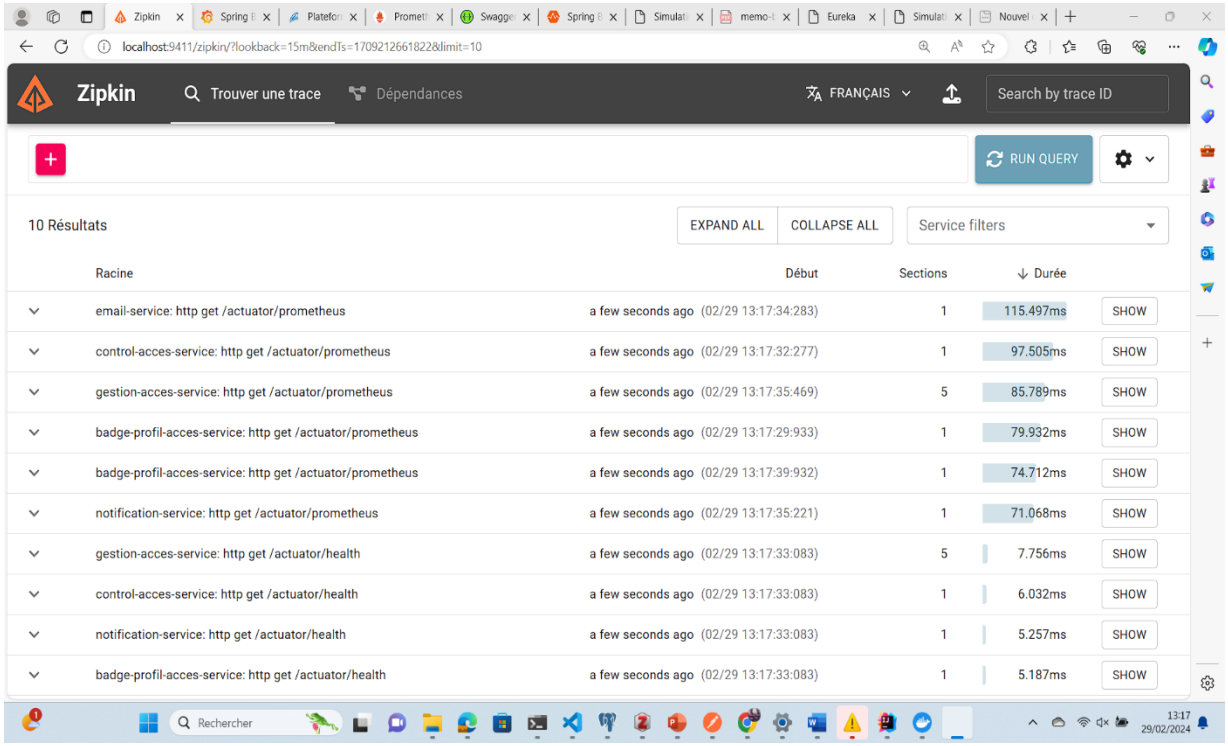


Figure 59 : Traçage avec Zipkin

Annexe 6 : Exemple de traçage de requête avec Zipkin

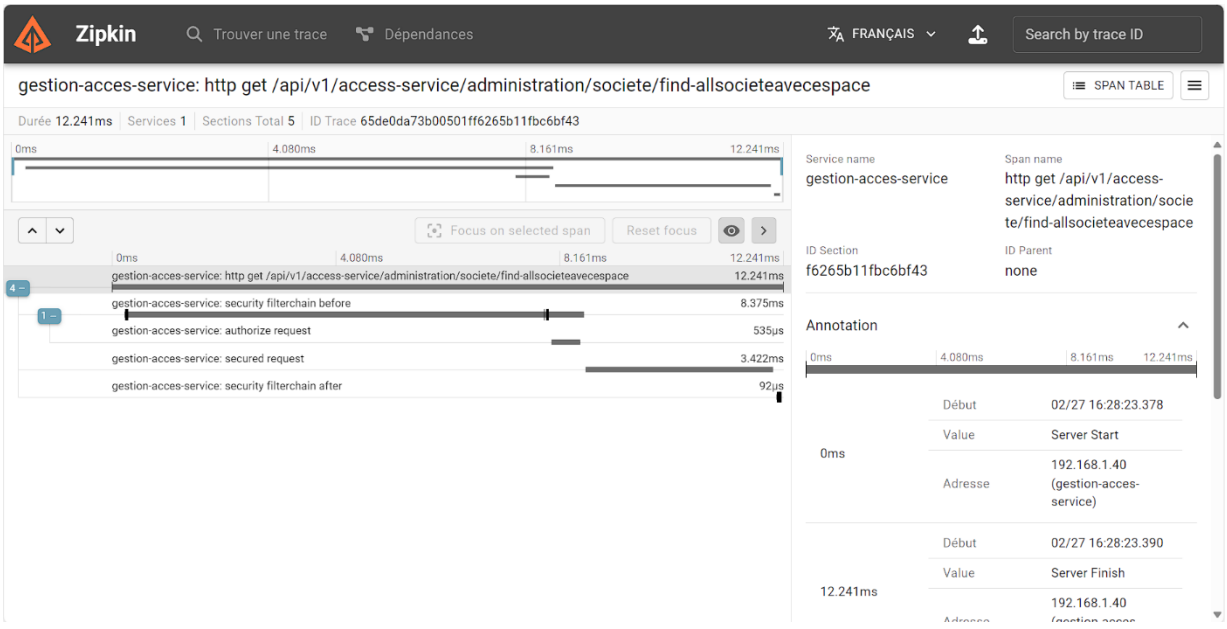


Figure 60 : Exemple de traçage d'une requête

Bibliographie

[1] A. Lalmi, S. Sassi Boudemagh, et G. Fernandes, « Le management de la qualité vers l'hybridation des méthodes en cascade et les méthodes agile », Thesis, Université Constantine 3 Salah Boubnider, Faculté d'architecture et d'urbanisme, 2021.

[2] C. Belleval, I. Filipas Deniaud, et C. Lerch, « MODELE DE CONCEPTION A BASE DE RESEAU DE CONTRADICTIONS. LE CAS DE LA CONCEPTION DES MICROSATELLITES AU CNES », janv. 2010.

[3] Z. Achour–Djelfa-Algérie, « Les méthodes de gestion de projet «agiles» Project management methods «agile» », *J. Sci. Int. Publ. Par*, vol. 8, nº 01, 2021.

[4] C. Khalil, « Les méthodes "agiles" de management de projets informatiques : une analyse "par la pratique" », phdthesis, Télécom ParisTech, 2011.

[5] H. Alaidaros, M. Omar, et R. Romli, « Towards an Improved Software Project Monitoring Task Model of Agile Kanban Method », vol. 7, p. 118-125, juin 2018.

[6] H. Koç, A. M. Erdoğan, Y. Barjakly, et S. Peker, « UML Diagrams in Software Engineering Research: A Systematic Literature Review », *Proceedings*, vol. 74, nº 1, Art. nº 1, 2021, doi: 10.3390/proceedings2021074013.

[7] K. Gos et W. Zabierowski, « The Comparison of Microservice and Monolithic Architecture », avr. 2020, p. 150-153. doi: 10.1109/MEMSTECH49584.2020.9109514.

[8] E. Vasilescu et S. Mun, « Service Oriented Architecture (SOA) Implications for Large Scale Distributed Health Care Enterprises », févr. 2006, p. 91-94. doi: 10.1109/DDHH.2006.1624805.

[9] V. Božić, *Microservices Architecture*. 2023. doi: 10.13140/RG.2.2.21902.84802.

[10] pstall, « système de contrôle d'accès », Dantila Technologies. Disponible sur: https://www.dantilatech.com/systeme-de-controle-d-acces/

[11] A. Haibi, K. Oufaska, K. E. Yassini, M. Boulmalf, et M. Bouya, « Systematic Mapping Study on RFID Technology », *IEEE Access*, vol. 10, p. 6363-6380, 2022, doi: 10.1109/ACCESS.2022.3140475.

[12] K. Aksa et M. Harrag, « Surveillance Des Zones Critiques Et Des Accès Non Autorisés En Utilisant La Technologie Rfid », juin 2022.

[13] A. Belhedri, R. Bouafia, et B. Bouafia, « Etude et conception d'une étiquette RFID à résonateur diélectrique dans la bande UHF », Thesis, UNIVERSITY OF KASDI MERBAH OUARGLA, 2023.

[14] A. Matallah, « Système De Controle D'Acces Physique », *Univ. Ahmed Draïa - Adrar*, janv. 2017.

[15] T. Kriplean *et al.*, « Physical Access Control for Captured RFID Data », *Pervasive Comput. IEEE*, vol. 6, p. 48-55, nov. 2007, doi: 10.1109/MPRV.2007.81.

[16] « Reconnaissance des plaques d'immatriculation (LPR) pour les parkings ». Disponible sur: https://www.skidata.com/fr/skidata-blog/reconnaissance-des-plaques-dimmatriculation-pour-les-parkings

[17] C. Patel, D. Shah, et A. Patel, « Automatic Number Plate Recognition System (ANPR): A Survey », *Int. J. Comput. Appl. IJCA*, vol. 69, p. 21-33, mai 2013, doi: 10.5120/11871-7665.

[18] A. Atanassov, « ADVANCED SOFTWARE ARCHITECTURE OF AN AUTOMATIC VEHICLE NUMBER PLATE RECOGNITION SYSTEM », 2012.

[19] « Gestion de Parking ANPR | Nortech Systèmes De Contrôle Ltée ». Disponible sur: https://www.nortechcontrol.com/solutions/vehicle/vehicle-access-with-counting-using-anpr/

[20] S. Alaoui Ismaili, « Big Data et reconnaissance des visages », masters, Université du Québec à Trois-Rivières, Trois-Rivières, 2022.