كلية العلوم و التقنيات فاس
ⵜⴰⵖⵙⵓⵍⵜ ⵏ ⵜⵜⵇⵏⵉⵜ ⴰⵏ ⵜⵎⵙⵙⵜⵉ
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵎⴰⵡⴰⵙⵜ ⵙⴰⵏ ⵎⵓⵃⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰ
Université Sidi Mohamed Ben Abdellah

Département d'Informatique

Projet de fin d'études

Master Sciences et Techniques
Systèmes Intelligents & Réseaux

Application décentralisée basée sur la blockchain pour la signature et la vérification des Documents (front-end)

التحول الذكي
Smart Transformation

Lieu du stage : SMART TRANSFORMATION

Réalisé par :

- Bouzidi Hamza

Encadré par :

- Pr. Adil Ben Abbou
- Pr. Abdelali Boushaba

Soutenu le 14.07.2021 devant le jury composé de :

- Pr. Rachid Ben Abbou	Faculté des Sciences et Techniques de Fès	(Examinateur)
- Pr. Fatiha Mrabti	Faculté des Sciences et Techniques de Fès	(Président)
- Pr. Adil Ben Abbou	Faculté des Sciences et Techniques de Fès	(Encadrant)
- Pr. Abdelali Boushaba	Faculté des Sciences et Techniques de Fès	(Encadrant)

Année Universitaire 2020 – 2021

Remerciement

Avec le plus grand honneur que je réserve cette page de gratitude et de reconnaissance à tous ceux qui ont contribué de près ou de loin au bon déroulement et à la réalisation de mon stage.

Je tiens à remercier les personnes qui m'ont permis de mener à bien ce projet de fin d'étude, ceux dont l'intervention a aidé et a favorisé son aboutissement.

Une pensée particulière est adressée tout spécialement à mes parents, mes frères, sœurs et amis qui m'ont toujours encouragé et soutenu lors de mon choix.

A cette occasion, j'exprime ma profonde gratitude et mon immense respect à Mr Adil Ben Abbou et Mr Abdelali Boushaba, mes encadrants à la faculté des sciences et techniques pour tous leurs conseils, leurs avis éclairés et leurs précieux soutien.

Un remerciement particulier aux membres du jury Pr Rachid Ben Abbou, Pr. Fatiha Mrabti pour avoir accepté de juger ce travail et de me faire profiter de leurs remarques et conseils.

Je tiens également à remercier Mr. EL KANDRI Mohamed le Directeur Général de la société SMART Transformation et Mme Nouhaila el Manioui, pour le suivi qu'ils ont apporté au projet, pour la sympathie, la disponibilité tout au long de mon stage de fin d'études.

Je voudrais remercier tout le personnel de SMART Transformation pour son soutien et bienveillance.

Je voudrais adresser toute ma gratitude à Mr ZAHI Azeddine chef du département pour le dynamisme de ce département d'études, à Madame A.Begdouri pour ses conseils, sa disponibilité durant cette période de pandémie, à tous les enseignants qui m'ont accompagnés durant ces années, pour leur gentillesse et leur efficacité, et pour la qualité de l'enseignement qui m'a été dispensée.

Résumé

La validation des documents constitue un obstacle majeur à l'échelle internationale, tenant compte des délais et procédures complexes qu'ils doivent endurer.

En outre, la fraude des diplômes et des certificats (tout autre type de document), constitue un risque majeur et n'a pas un impact seulement sur la crédibilité du système d'éducation mais aussi pour le simple citoyen.

Par exemple, cet obstacle peut être posé aux recruteurs qui peuvent recevoir plusieurs candidatures et n'ont pas accès à un outil efficace afin de confirmer l'authenticité des documents des candidats.

L'objectif de ce travail est la signature et la vérification automatique des documents en maximisant la sécurité afin d'éviter toute difficulté rencontrée lors de la réutilisation de ces documents et aussi éliminer le risque de fraude.

Mots clés : Blockchain, diplôme, étudiant, signature, vérification, université, recruteur.

Abstract

The validation of documents is a major obstacle at the international level, taking into account the delays and complex procedures they have to endure.

In addition, the fraud of diplomas and certificates (or any other type of document) constitutes a major risk and has an impact not only on the credibility of the education system but also for the ordinary citizen.

For example, this obstacle can be posed to recruiters who may receive several applications and do not have access to an efficient tool to confirm the authenticity of the candidates' documents.

The objective of this work is the automatic signature and verification of documents by maximizing the security in order to avoid any difficulty encountered during the reuse of these documents and also eliminate the risk of fraud.

Keywords: Blockchain, diploma, student, signature, verification, university, recruiter.

Table des matières

Liste des figures

Liste des tableaux

Introduction Générale

À une époque où les informations sont démultipliées et disponibles sous différents médias, se doter de systèmes automatiques de traitement de ces informations devient primordial, or il est important de réfléchir au développement de référentiels communs permettant de qualifier la fiabilité de ces systèmes de traitement automatique de l'information et d'assurer leur traçabilité du point de vue de l'analyse de la performance et du contrôle qualité.

Par exemple Les méthodes classiques pour la gestion des diplômes/attestations universitaires engendrent plusieurs problèmes chez les jeunes diplômés. Nous pouvons citer comme exemples :

- La perte du temps lors de la vérification des diplômes qui peut prendre des semaines dans certains cas.

- Dans le cas de perte d'un document scolaire (ex. Baccalauréat), la personne n'a pas le droit à une autre copie et cela pose un problème de sécurité lors du déplacement de ce document.

- Si une personne a besoin d'utiliser son document officiel plusieurs fois, elle est dans l'obligation de fournir des copies certifiées et cela cause de la perte de temps.

- Prouver la véracité d'un document dans le cas de quelques sociétés étrangères peut s'avérer une tâche très compliquée.

Donc le but de résoudre ces problèmes, la société Smart Transformation a proposé la réalisation d'une application décentralisée basée sur la technologie Blockchain, qui assure la signature, la vérification, la sécurité et la facilité de la gestion des documents officiels.

- **Le premier chapitre** présente le contexte général du projet comportant une présentation de l'organisme d'accueil, le cadre du projet, ses objectifs.
- **Le deuxième chapitre** décrit état de l'art de la Blockchain
- **Le troisième chapitre** décrit le contexte global du projet, ainsi que la description des besoins fonctionnels, et aussi l'analyse et la conception.
- **Le quatrième chapitre** est consacrée à la présentation des outils et les technologies utilisées dans la réalisation ainsi que la présentation des interfaces de l'application développée.

Chapitre 1 contexte général du projet

Introduction

Dans ce chapitre, nous présentons notre organisme d'accueil du stage, par la suite, nous faisons une étude de l'existant afin de relever les insuffisances et de proposer une solution efficace.

1. Présentation de l'organisme d'accueil.

1.1. Présentation de l'entreprise

Smart Transformation est une entreprise technologique de renommée, née de la passion des nouvelles technologies telles que Blockchain, AI et IoT.

Depuis la création de Smart Transformation l'objectif principale qui vise principalement à le réaliser est d'utiliser des technologies de pointe pour développer des solutions futuristes.

La mission de Smart Transformation concerne plusieurs axes tels que :

- Développement
- Applications décentralisées
- Développement de contrat intelligent
- Développement d'application web
- Déploiement d'application

Smart Transformation occupe une position mondiale en tant que partie intégrante de la Dhahran Techno Valley : un parc scientifique de premier plan regroupant des sociétés géantes telles qu'ARAMCO, SIPCHEM, Schlumberger et Honeywell, où elle collabore étroitement avec ses partenaires en Arabie saoudite pour favoriser la transformation numérique dans le secteur de L'industrie pétrolière et gazière.

Smart Transformation collaborent aussi étroitement avec l'Université Roi Fahd du pétrole et des minéraux - KFUPM (Qui occupe la Septième place mondiale en ce qui concerne le nombre de brevets délivrés par l'Office des brevets américain aux universités) afin de mettre au point

un système de certification intelligent. Smart Transformation compte aussi plusieurs partenaires stratégiques au Canada.

Smart Transformation a également ouvert des bureaux au Maroc afin de renforcer les capacités locales, de participer à la transformation numérique en cours dans le pays et de faire le transfert de l'expertise internationale pour accélérer cette transformation.

1.2. Organigramme

L'organigramme illustré dans la figure 2 ci-dessous, représente la structure hiérarchique de Smart Transformation Maroc :

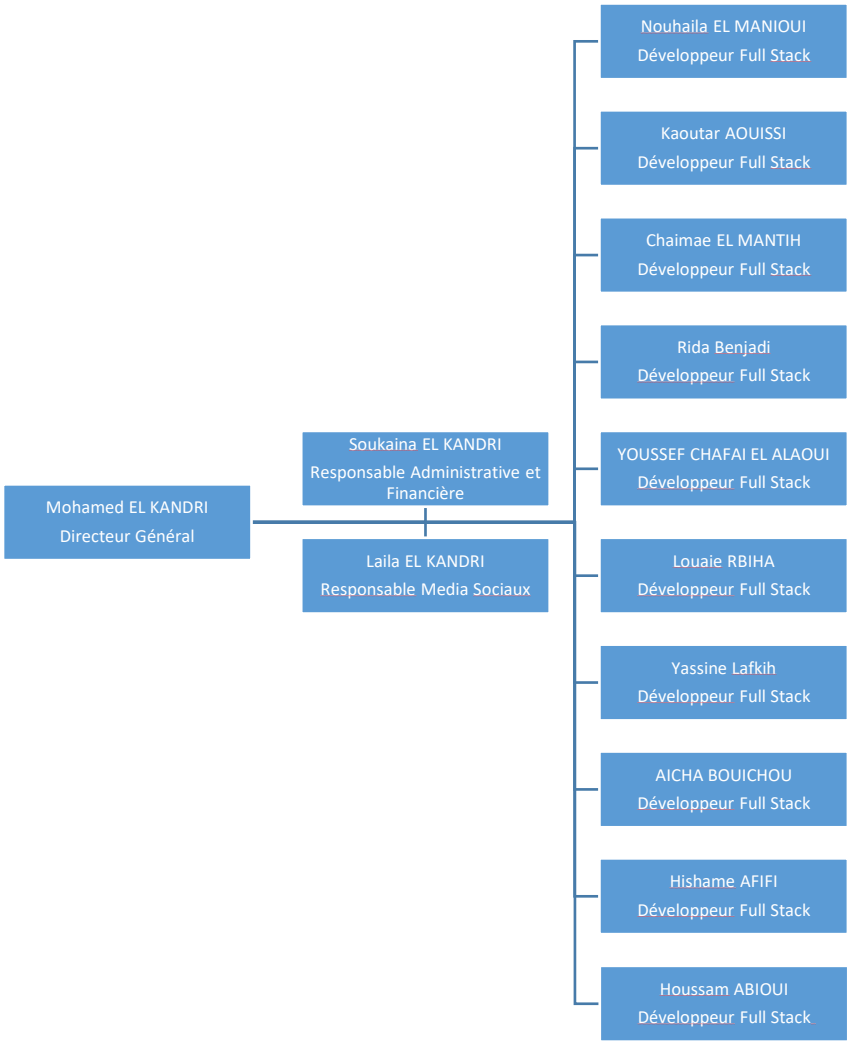


Figure 1 Organigramme de Smart Transformation Maroc

1.3. Contexte du projet

1.3.1. **Problématique**

Les méthodes classiques pour la gestion des documents officiels posent nombreux problèmes,

Parmi eux nous pouvons citer :

- Les personnes n'ont pas accès à une nouvelle copie dans le cas d'une perte de certains documents officiels (ex. Baccalauréat). Ce qui pose un problème de manque de sécurité lors d'un simple déplacement du diplôme.
- La grande perte du temps dans la préparation des copies certifiées des documents.
- Dans certains cas, les personnes peuvent trouver des problèmes et des difficultés à prouver l'authenticité de leurs documents par d'autres établissements étrangers.
- La société recevant le document doit vérifier la véracité du document, et cela pose aussi un problème de perte de temps.
- Le temps est perdu dans la préparation des copies certifiées des diplômes, ce qui n'est pas très pratique dans des cas urgents.
- La gestion actuelle des diplômes pose aussi des problèmes pour les universités, l'université doit gérer la charge du travail pour vérifier les diplômes (Via téléphone, e-mail ou courrier) ainsi l'établissement perd du temps afin de vérifier les candidats potentiels.

1.3.2. **Solution proposée**

Pour résoudre les problèmes cités, la société Smart Transformation en collaboration avec l'université KING FAHD du pétrole et minéraux « KFUPM » Arabie Saoudite ont proposé de mettre en place une solution qui permet la signature automatique des documents et aussi leurs vérifications rapides par n'importe quel établissement.

Ce projet a pour objectif :

- La signature automatique des documents, ce qui rend le processus de certification plus rapide, plus fiable et plus pratique.
- Le Stockage des informations des documents de façon décentralisée sur la Blockchain et peuvent être traqués facilement, et cela augmente le niveau de sécurité par rapport aux techniques classiques.
- La vérification des documents se fait d'une manière automatique, ce qui est plus rapide, instantanée et ne nécessite aucune intervention externe grâce à la Blockchain, et cela rend le document reconnu partout.

- La personne peut déposer son dossier facilement chez n'importe quelle société dans le monde, et cette dernière vérifie instantanément l'authenticité de ces documents.
- L'administrateur de chaque réseau donne un accès sécurisé à chaque utilisateur souhaitant accéder son réseau soit pour recevoir ou vérifier un document.

Voici ci-dessous un schéma décrivant le processus de la signature d'un document d'un utilisateur et sa vérification :

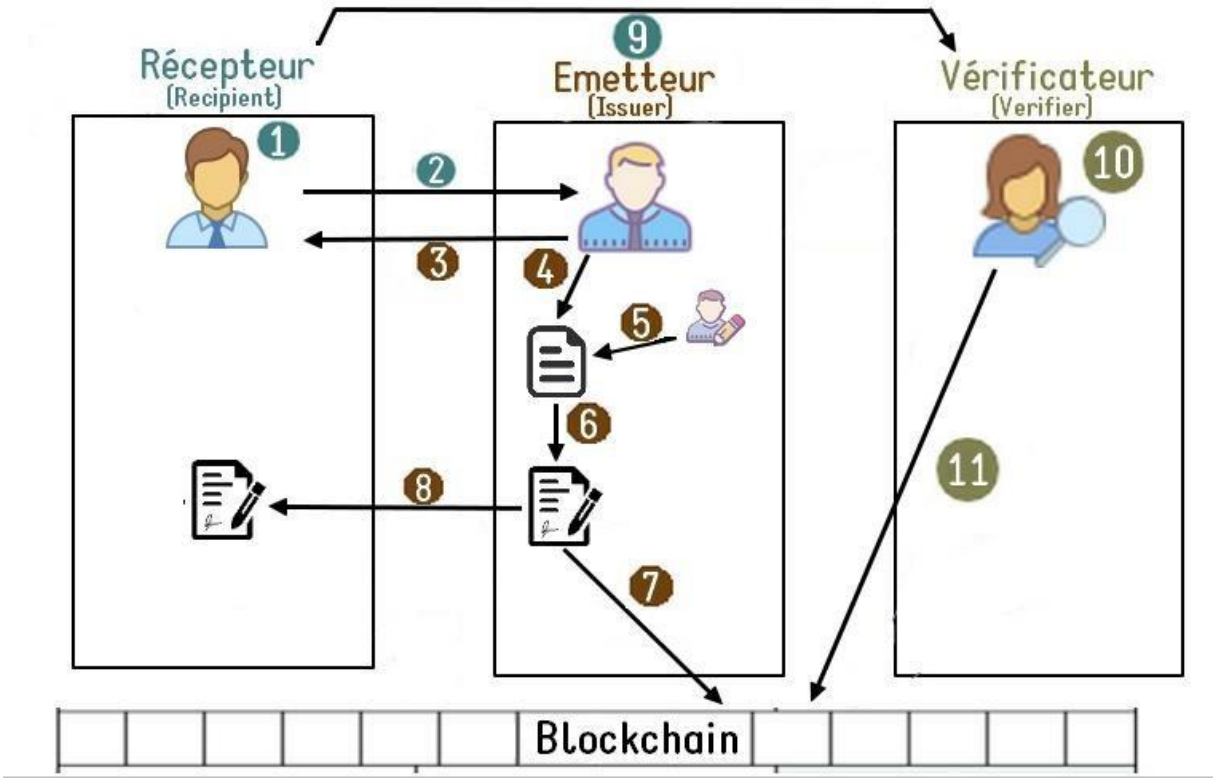


Figure 2 : processus de la signature et vérification d'un document

1 : L'utilisateur effectue l'enregistrement en tant que récepteur.

2 : Envoie automatique d'une demande à l'administrateur de l'organisme pour la validation de l'enregistrement effectuée.

3 : Emetteur peut approuver l'enregistrement ou non (On suppose qu'il l'a accepté)

4 : Emetteur créer le document associé à la personne.

5 : Le document va être vérifié par les signataires affectés à ce document par Emetteur.

6 : Le document va être signé par Emetteur lui-même.

7 : Le document est publié sur la Blockchain d'une manière permanente

8 : Le récepteur reçoit son certificat.

9 : Le récepteur peut partager l'ID de son certificat avec un vérificateur quelconque

10 : Le vérificateur effectue l'enregistrement en tant que vérificateur.

11 : Après l'acceptation de la part de Emetteur, le vérificateur peut commencer le processus de vérification du document dans la Blockchain en utilisant l'ID fourni de la part du récepteur.

Conclusion

Ce chapitre a été consacré au début à une présentation de l'organisme d'accueil, ensuite nous avons donné la description du problème posé et nous avons ainsi défini les différents objectifs de notre application.

Chapitre 2 État de l'art de la blockchain

Introduction

Le 31 octobre 2008, un inconnu utilisant le pseudonyme « Satoshi Nakamoto » a écrit dans une liste de diffusion d'e-mails réservée aux cypherpunks (un mouvement de personnes utilisant la cryptographie pour protéger la vie privée). : "Je travaille sur un nouveau système de monnaie électronique entièrement de pair-à-pair, sans tiers de confiance". Ce texte est accompagné d'un lien qui amène vers Bitcoin.org et sur lequel est hébergé le livre blanc du Bitcoin, rédigé dans un anglais impeccable, résumant le fonctionnement du nouveau protocole. Le premier concept de Blockchain a été appliqué le 03 janvier 2009 dans le cadre de Bitcoin.

La technologie à la base de Bitcoin et d'autres crypto-monnaies, est une base de données de grand livre distribuée pour l'enregistrement des transactions, permettant ainsi aux utilisateurs de partager leur grand livre de transactions.

Dans ce chapitre, On présente et on explique la technologie Blockchain avec ses fonctionnalités les plus importantes et ses concepts associés.

1. Utilisation de la blockchain

Les blockchains sont utilisées lorsque plusieurs parties, peut-être situées à travers le monde, ont besoin de partager des données et de transférer de la valeur sans se faire confiance.

Le monde financier décrit cette confiance comme le risque de contrepartie : le risque que l'autre partie ne tienne pas sa part du marché. Les blockchains éliminent complètement le risque de contrepartie grâce à un système révolutionnaire de mathématiques, de cryptographie et de mise en réseau peer-to-peer.

2. Evolution de la Blockchain

En 2009, l'évolution de la blockchain a commencé avec le concept en développement de « l'économie entre homologues » sur Internet, connu sous le nom de Bitcoin. Le bitcoin est fourni et pris en charge, pas par une autorité centrale, par ex. Banque ou entreprise comme PayPal, mais par consentement automatique entre utilisateurs du réseau. Son caractère unique repose toutefois sur le fait que les utilisateurs ne devaient pas se faire confiance. Grâce à l'auto-contrôle algorithmique, toute tentative malveillante de tromper le système est interdite. Techniquement, le bitcoin est une monnaie numérique qui est traitée via Internet dans un système décentralisé sans confiance utilisant un registre public appelé blockchain. Il combine le partage de fichiers peer-to-peer entre BitTorrent et la cryptographie à clé publique.

Les Avantages de la blockchain ne se limitent pas à l'économie entre pairs. Ils s'étendent aux domaines politique, environnemental, médical, etc. Par exemple :

- Pour lutter contre les systèmes politiques oppressifs, la technologie blockchain peut être utilisée pour intégrer dans un cloud décentralisé des fonctions qui, auparavant, nécessitaient une administration par des organisations juridiquement responsables.

- La coordination, la tenue des registres et l'irrévocabilité des transactions utilisant la technologie de la blockchain sont des caractéristiques qui pourraient être aussi essentielles au progrès de la société que la Magna Carta ou la Rosetta Stone. Dans ce cas, la blockchain peut servir de référentiel d'archives publiques pour des sociétés entières, y compris le registre de tous les documents, événements, identités et actifs. Dans ce système, toute propriété pourrait devenir une propriété intelligente ; c'est la notion d'encoder chaque actif dans la blockchain avec un identifiant unique permettant de suivre, contrôler et échanger (acheter ou vendre) l'actif sur la blockchain. Cela signifie que toutes sortes d'actifs corporels (maisons, voitures) et numériques peuvent être enregistrés et traités sur la blockchain [1].

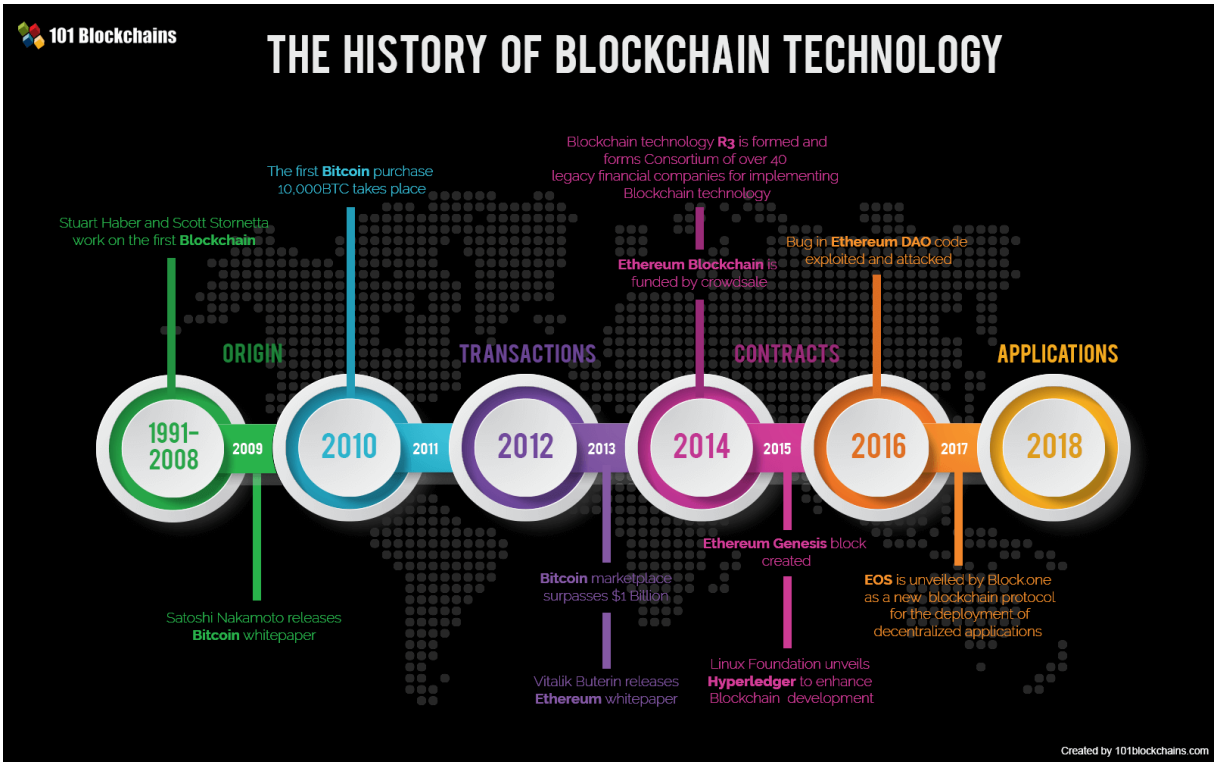


Figure 3 : Historique de la technologie Blockchain [16]

2.1. Les premières bases de données

Les premières bases de données informatisées ont vu le jour dans les années 1960. Comme le matériel informatique occupait plusieurs pièces et qu'Internet n'existait pas encore depuis des décennies, les données se trouvaient naturellement dans des emplacements physiques centraux. Il s'agit d'une approche centralisée, ce qui signifie que l'emplacement et l'accès aux données sont contrôlés par une autorité centrale.

Les systèmes centralisés peuvent être manipulés, de l'intérieur ou de l'extérieur, et nous devons donc faire confiance à la volonté et aux ressources des propriétaires de ces systèmes pour assurer la sécurité et l'intégrité de leurs données. Les bases de données centralisées sont encore les plus courantes aujourd'hui, elles alimentent la plupart de nos applications en ligne et hors ligne.

Un blog auto-hébergé est un exemple courant de base de données centralisée. Le propriétaire peut potentiellement modifier les messages a posteriori ou censurer les utilisateurs sans recours. Ou encore, un pirate informatique pourrait s'infiltrer dans le serveur et commettre des actes malveillants. S'il n'y a pas de sauvegarde de la base de données, il peut être impossible de réparer les dégâts [2].

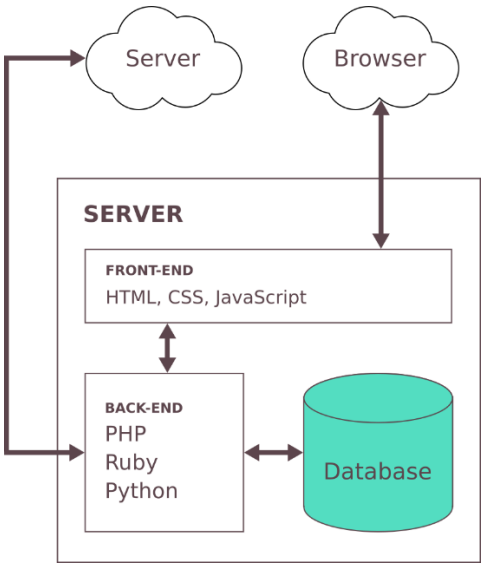


Figure 4 : base de données-serveur [16]

2.2. Le besoin de partager des données

Le partage de grandes quantités de données peut être coûteux et fastidieux. Nous pouvons alléger ce fardeau en distribuant les données entre plusieurs parties. La lecture et l'écriture sont contrôlées par une ou plusieurs parties au sein du groupe et sont donc sujettes aux mêmes corruptions que les bases de données centralisées.

Les bases de données partagées modernes utilisent des techniques pour minimiser cette corruption. Certaines de ces techniques se recoupent avec les blockchains. Selon le système de base de données partagée, elle peut présenter les caractéristiques suivantes :

- **Immutabilité** : Plutôt que d'écraser les anciennes données, une nouvelle copie est créée, les anciennes données étant conservées comme un enregistrement historique. Cet enregistrement peut être consulté pour prouver qu'un élément de données a existé à un moment donné.
- **Consensus** : Pour qu'une base de données puisse être partagée, toutes les parties doivent être d'accord sur son contenu. Il existe plusieurs méthodes pour parvenir à un consensus, l'une d'entre elles (preuve de travail) sera abordée ci-dessous.

Les blockchains les utilisent et les poussent encore plus loin, résolvant le problème de la confiance.

3. Définition de la blockchain

Fondamentalement, une blockchain [3] est une base de données partagée, constituée d'un grand livre des transactions. À l'instar d'une banque, les grands livres des blockchains simples gardent la trace de la propriété des devises (dans ce cas, les crypto-monnaies). Contrairement à une banque centralisée, chacun dispose d'une copie du grand livre et peut vérifier les comptes des autres. Chaque appareil connecté possédant une copie du grand livre est appelé "nœud".

Les blockchains éliminent le problème de confiance qui affecte les autres bases de données de la manière suivante :

- Décentralisation complète : La lecture/écriture dans la base de données est entièrement décentralisée et sécurisée. Aucune personne ou groupe ne contrôle une blockchain.
- Tolérance extrême aux pannes : La tolérance aux pannes est la capacité d'un système à gérer des données corrompues. Bien que la tolérance aux pannes ne soit pas propre aux blockchains, elle pousse le concept à son extrême logique en faisant valider ses modifications par chaque compte partageant la base de données.

- Vérification indépendante : Les transactions peuvent être vérifiées par n'importe qui, sans l'intervention d'un tiers. C'est ce qu'on appelle parfois la "désintermédiation".

3.1. Le fonctionnement de la blockchain

Les interactions entre les comptes d'un réseau blockchain sont appelées "transactions". Il peut s'agir de transactions monétaires, comme l'envoi d'éther, la crypto-monnaie utilisée dans Ethereum. Elles peuvent également être des transmissions de données, comme un commentaire ou un nom d'utilisateur. Un ensemble de transactions est appelé un "bloc".

Chaque compte sur la blockchain possède une signature unique, qui permet à chacun de savoir quel compte a initié la transaction. Sur une blockchain publique, tout le monde peut lire ou écrire des données. La lecture des données est gratuite, mais l'écriture sur la blockchain publique est payante. Ce coût, appelé "gaz" et fixé en éther, contribue à décourager le spam et à sécuriser le réseau.

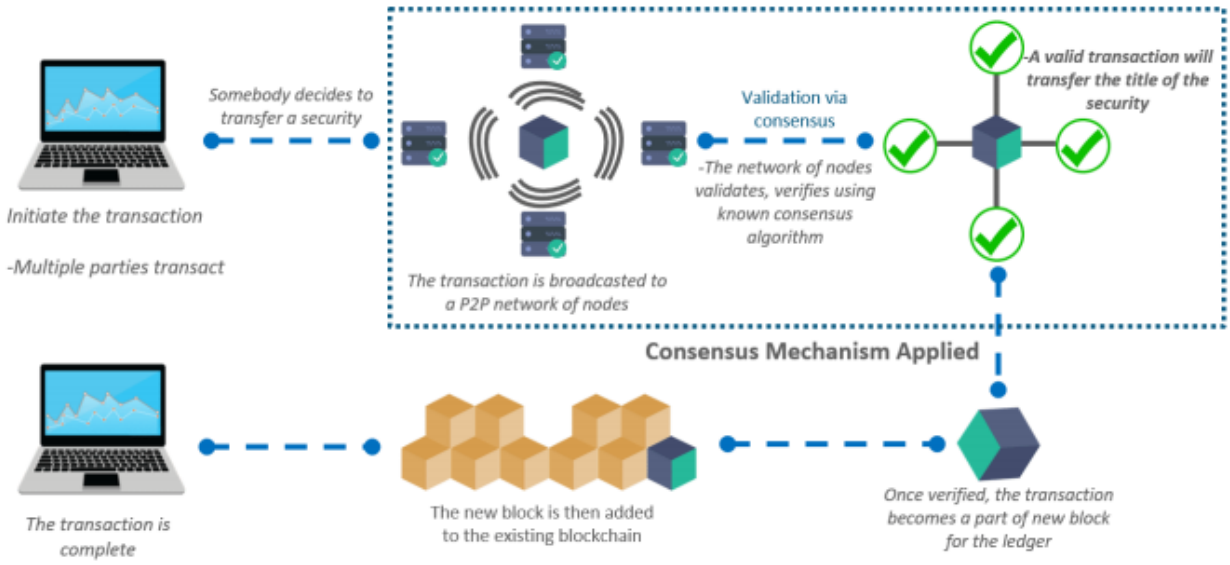


Figure 5 : Les étapes sur un réseau Blockchain

La figure 6 illustre le mécanisme de fonctionnement des transactions dans le réseau Blockchain [4].

Les étapes de ce mécanisme sont les suivantes :

- Quelqu'un demande une transaction.

- La transaction est diffusée sur un réseau P2P public (réseau Blockchain) composé de plusieurs nœuds.

- Le réseau de nœuds valide la transaction en utilisant les algorithmes de hachage.

- Une fois vérifiée, la transaction est combinée avec d'autres transactions pour créer un nouveau bloc de données pour le grand livre.

- Le nouveau bloc est ajouté à la chaîne de blocs existante, sous une forme qui est permanente et inaltérable.

- Enfin la transaction sera effectuée avec succès.

3.1.1. **Minage (Mining)**

Tout nœud du réseau peut participer à la sécurisation du réseau par un processus appelé "minage". Les nœuds qui ont choisi d'être des mineurs sont en concurrence pour résoudre des problèmes mathématiques qui sécurisent le contenu d'un bloc.

Comme le minage [5] nécessite de la puissance de calcul (sans parler du coût de l'électricité), les mineurs peuvent être rémunérés pour leur service. Le gagnant de la compétition reçoit des crypto-monnaies en guise de récompense. Cela incite les nœuds à travailler à la sécurisation du réseau, en évitant que trop de puissance ne soit entre les mains d'un seul mineur.

3.1.2. **Hachage**

Dès qu'un nouveau bloc est extrait, les autres mineurs en sont informés et commencent à vérifier et à ajouter ce nouveau bloc à leur copie de la chaîne. Cette opération s'effectue par hachage [6] cryptographique (ou simplement "hachage"). Le hachage est un processus à sens unique qui prend des données et renvoie une chaîne de longueur fixe représentant ces données.

Si les données originales ne peuvent être reproduites à partir de leur hachage, les mêmes données produiront toujours le même hachage. Par conséquent, les données non vérifiées peuvent être hachées avec la même fonction et comparées à l'original. Si elles sont identiques, les données sont validées.

Une fois que plus de la moitié des mineurs ont validé le nouveau bloc, le réseau a "atteint un consensus" et le bloc fait partie de l'histoire permanente de la blockchain. Ces données peuvent désormais être téléchargées par tous les nœuds, leur validité étant assurée.

Voici l'ensemble du processus visuellement :

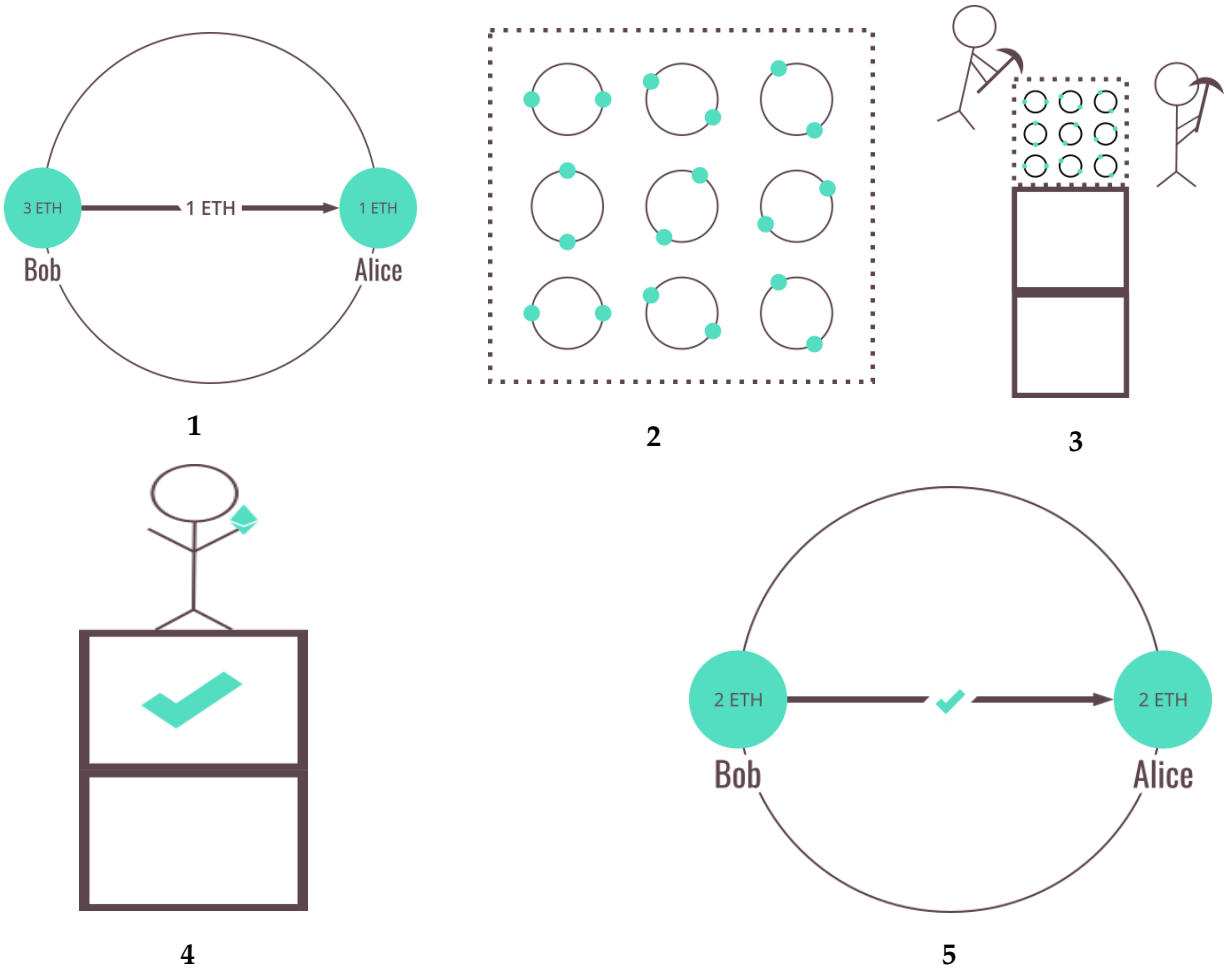


Figure 6: processus de minage de la blockchain [16]

1- Bob tente d'envoyer à Alice 1 ETH

2- La transaction de Bob et Alice est combinée avec d'autres transactions qui ont eu lieu depuis le dernier bloc

3- Les mineurs sont en concurrence pour valider le bloc avec le nouvel ensemble de transactions

4- Le mineur victorieux crée un nouveau bloc et reçoit une récompense

5- Une fois la transaction validée, Alice reçoit 1 ETH

4. Ethereum

Ethereum est une blockchain qui vous permet d'exécuter des programmes dans son environnement de confiance. Cela contraste avec la blockchain Bitcoin, qui ne vous permet que de gérer des crypto-monnaies.

À cette fin, Ethereum dispose d'une machine virtuelle, appelée Ethereum Virtual Machine (EVM). L'EVM permet de vérifier et d'exécuter du code sur la blockchain, en garantissant qu'il sera exécuté de la même manière sur la machine de chacun. Ce code est contenu dans des "contrats intelligents".

Au-delà du simple suivi des soldes de comptes, Ethereum maintient l'état de l'EVM sur la blockchain. Tous les nœuds traitent les contrats intelligents pour vérifier l'intégrité des contrats et de leurs résultats.

5. Smart contract

Un contrat intelligent est un code qui s'exécute sur l'EVM. Les contrats intelligents peuvent accepter et stocker de l'éther, des données ou une combinaison des deux. Ensuite, en utilisant la logique programmée dans le contrat, il peut distribuer cet éther à d'autres comptes ou même à d'autres contrats intelligents.

Voici un exemple de contrat intelligent avec Bob et Alice. Alice veut engager Bob pour lui construire un patio, et ils utilisent un contrat de séquestre (un endroit où stocker de l'argent jusqu'à ce qu'une condition soit remplie) pour stocker leur éther avant la transaction finale.

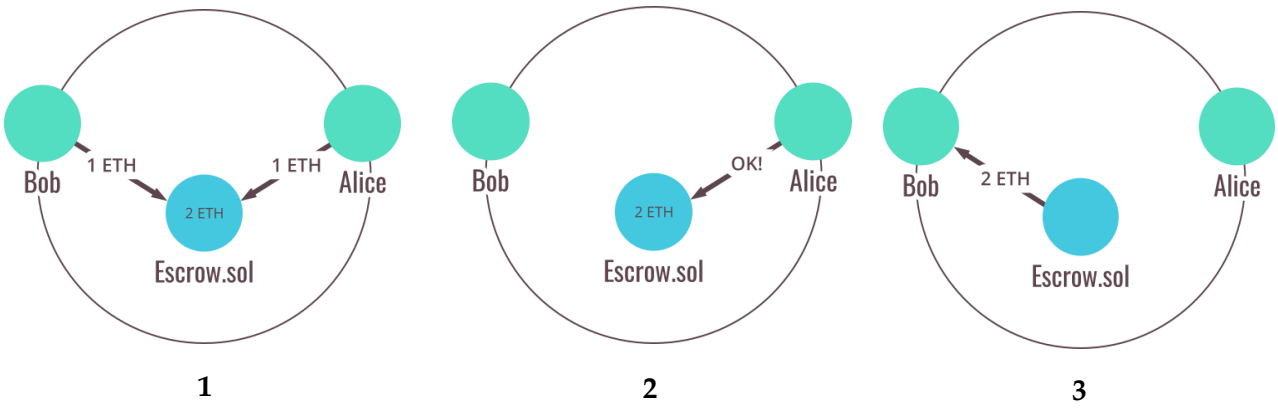


Figure 7: exemple de contrat intelligent [16]

1. Alice accepte de stocker son paiement pour le patio dans le contrat d'entiercement, et Bob accepte de déposer un montant égal.
2. Bob termine le projet de patio et Alice autorise le contrat intelligent à débloquer les fonds.

3. Bob reçoit le paiement d'Alice avec sa garantie.

Les contrats intelligents sont écrits dans un langage appelé Solidity. Solidity est typée statiquement et prend en charge, entre autres, l'héritage, les bibliothèques et les types complexes définis par l'utilisateur. La syntaxe de Solidity est similaire à celle de JavaScript.

6. Réseaux de test publics

Les données de la chaîne - y compris les soldes des comptes et les transactions - sont publiques, et n'importe qui peut créer un nœud et commencer à vérifier les transactions. Sur ce réseau, l'Ether a une valeur marchande et peut être échangé contre d'autres crypto-monnaies ou des monnaies fiduciaires comme le dollar américain.

Il existe trois réseaux de test publics largement utilisés :

- **Ropsten** : Le réseau de test officiel, créé par la Fondation Ethereum. Sa fonctionnalité est similaire à celle du MainNet.
- **Kovan** : Un réseau qui utilise une méthode de consensus appelée "proof-of-authority". Cela signifie que ses transactions sont validées par des membres sélectionnés, ce qui conduit à un temps de blocage constant de quatre secondes. L'approvisionnement en éther sur ce réseau de test est également contrôlé pour limiter les attaques de spam.
- **Rinkeby** : Un testnet utilisant également la preuve d'autorité, créé par la Fondation Ethereum.

7. Réseaux privés / d'entreprise

Les réseaux Ethereum privés permettent aux parties de partager des données sans les rendre accessibles au public. Une blockchain privée est un bon choix pour :

- Le partage de données sensibles, comme les dossiers de soins de santé.
- La mise à l'échelle pour gérer un débit de lecture/écriture plus élevé, en raison de la taille réduite du réseau.

8. Applications décentralisées

Les applications qui utilisent des contrats intelligents pour leur traitement et/ou leur stockage de données sont appelées "applications décentralisées", ou "dapps". Les interfaces utilisateur de ces dapps sont constituées de langages familiers tels que HTML, CSS et JavaScript. L'application elle-même peut être hébergée sur un serveur web traditionnel ou sur un service de fichiers décentralisé tel que Swarm ou IPFS.

Compte tenu des avantages de la blockchain Ethereum, une dapp pourrait être une solution pour de nombreux secteurs d'activité, notamment, mais sans s'y limiter :

- Tenue de registres
- La finance
- Des chaînes d'approvisionnement
- Immobilier
- Marchés

8.1. Applications de la Blockchain

Dans cette section, On présente certaines des applications potentielles de la technologie Blockchain [7], Ces applications sont Chaîne d'approvisionnement, identité numérique, vote, santé et gouvernement.

Chaîne d'approvisionnement : La chaîne d'approvisionnement est un segment très complexe et il est devenu plus difficile d'avoir une visibilité transparente sur l'ensemble de la chaîne d'approvisionnement. Il est devenu plus difficile de suivre le flux de matériel et les canaux de distribution, ce qui a entraîné divers comportements contraires à l'éthique dans les entreprises, allant du commerce illégal aux produits de contrefaçon et aux dommages environnementaux.

Tout au bout de la chaîne d'approvisionnement, les consommateurs ne disposent pas des informations selon lesquelles un produit final a été importé tout au long de la chaîne d'approvisionnement. De nos jours, vous pouvez perdre vos colis par la poste. En tirant parti de la convergence du paradigme IoT et des contrats intelligents, vous pourrez enregistrer la position à tout moment de vos colis grâce à la connexion de capteurs à chaque étape.

Le contrat intelligent : apporte la fiabilité tout au long de la ligne, permettant avec sécurité où trouver le paquet. -Identité numérique. Cette application pourrait permettre aux consommateurs d'avoir une identité enregistrée sur un grand livre partagé et d'ajouter des appareils à leur identité.

L'identité numérique : garantit un moyen plus sûr de vérifier l'authenticité d'une personne et d'éviter et de réduire les fraudes possibles.

Certificat numérique : garantit un moyen plus sûr de signer et de vérifier l'authenticité des documents d'une manière automatique ce qui est plus rapide et plus.

Vote : Blockchain peut transformer le système de vote traditionnel sur papier en un système numérisé et peut fournir une plate-forme de vote sécurisée servant de support à tout le processus ; voter, dépister et compter les votes et éviter des problèmes tels que la perte de registres et la fraude électorale. Les électeurs pouvaient compter les votes eux-mêmes et vérifier qu'aucun vote n'avait été supprimé, manipulé ou modifié.

Gouvernement : La blockchain pourrait être utilisée pour assurer au public que les politiciens agissent correctement avec l'argent, et peut également lutter contre le crime financier. Grâce à la technologie, chaque transaction peut être enregistrée sans manipulation, ce qui rend la destination ultime transparente pour le public.

Santé : Les établissements de santé doivent faire face à des problèmes de sécurité et de confidentialité lorsqu'ils partagent des données sur plusieurs plates-formes. L'amélioration de la collaboration de données entre fournisseurs signifie l'amélioration de nombreux aspects du domaine de la santé, tels que la précision des diagnostics et l'efficacité des traitements. Blockchain peut créer cet environnement sécurisé pour permettre aux établissements de santé, aux payeurs et aux autres acteurs de ce domaine de partager l'accès à leur réseau avec des garanties d'intégrité des données.

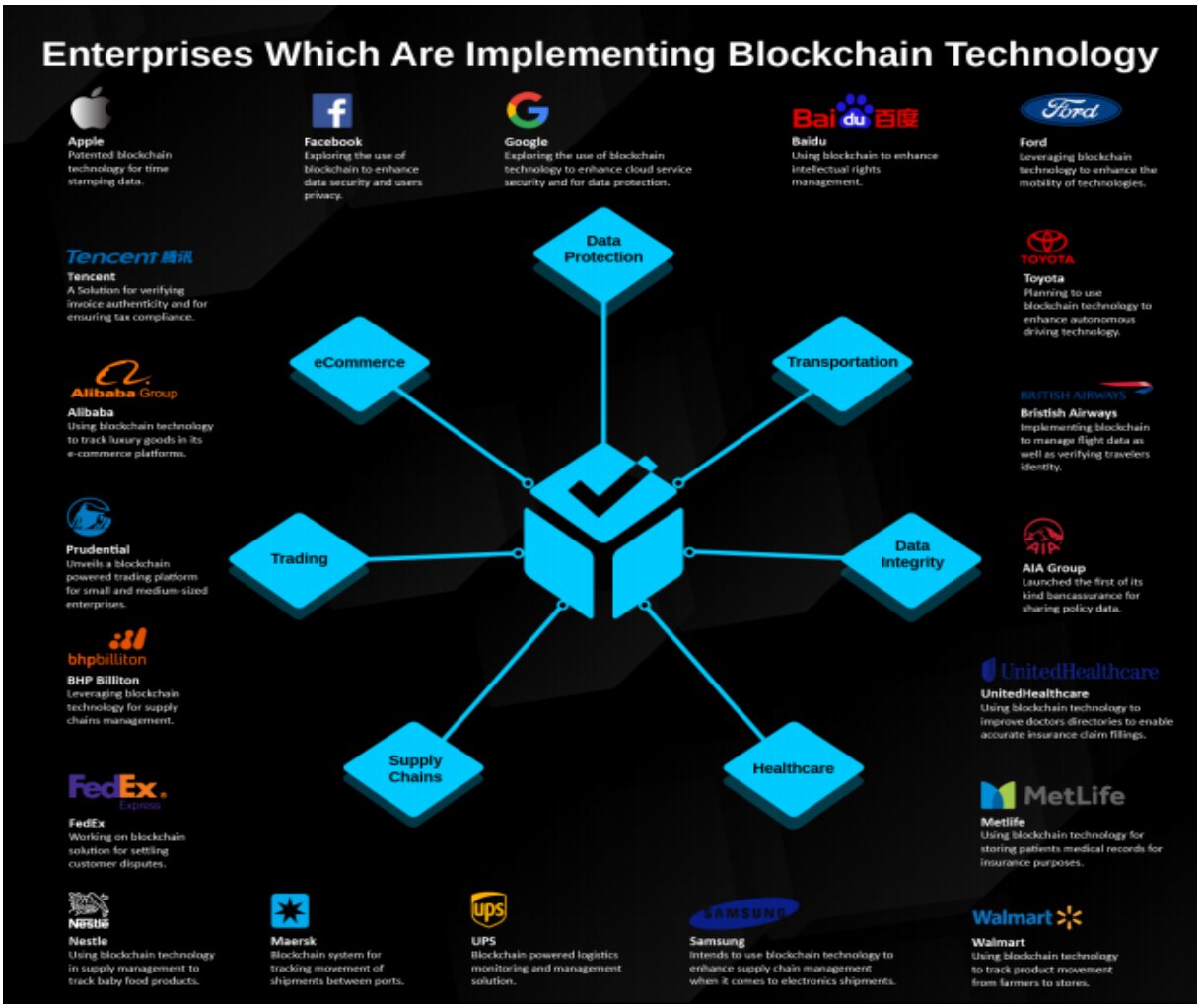


Figure 8 : Entreprises implémentant la Blockchain [17].

9. Défis de la Blockchain

La blockchain est une technologie émergente qui se répand dans divers secteurs et qui présente un grand nombre d'avantages et d'opportunités. Cependant, cette technologie présente son propre ensemble de défis [8] à relever. Quelques-uns de ces défis majeurs sont abordés dans cette section.

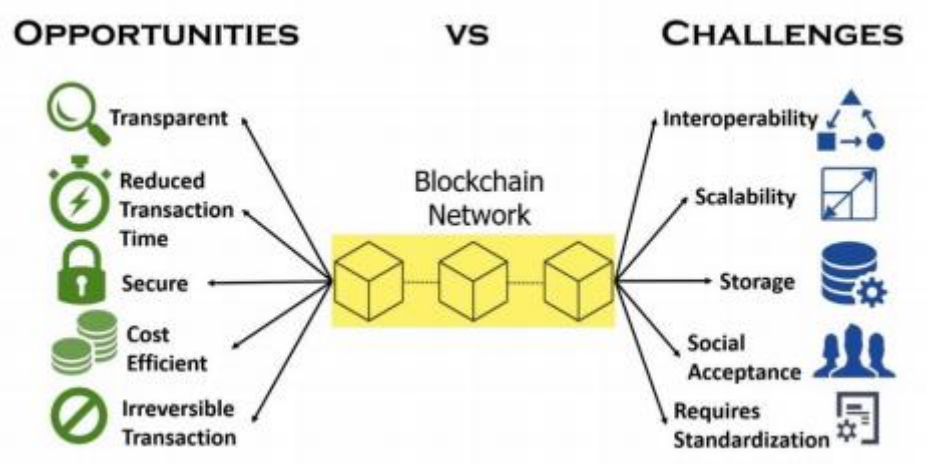


Figure 9: Opportunités et défis des blockchains [8]

Source: Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives.

Sécurité et confidentialité des données

Le premier et le plus important défi concerne la sécurité et la confidentialité des données. Avec la mise en œuvre d'applications basées sur la technologie de la blockchain, la nécessité pour un tiers d'effectuer une transaction est éliminée. Étant donné que le mécanisme de blockchain permet à l'ensemble de la communauté, plutôt qu'à un seul tiers de confiance, de vérifier les enregistrements dans une architecture de blockchain, les données sont exposées à des risques potentiels en matière de sécurité et de confidentialité. Étant donné que tous les nœuds peuvent accéder aux données transmises par un nœud, la confidentialité des données ne sera pas active.

En cas d'absence d'une tierce partie pour autorisation, le patient doit sélectionner un ou plusieurs représentants qui peuvent accéder à ses informations et / ou à ses antécédents médicaux en son nom, en cas d'urgence. Désormais, ce représentant peut également autoriser un ensemble de personnes à accéder aux enregistrements du même patient, ce qui peut créer une menace énorme pour la sécurité et la confidentialité des données. L'implication de mécanismes de haute sécurité dans les données entraînera à son tour des obstacles pour le transfert des données d'un bloc à un autre et, par conséquent, les destinataires auront accès à des données limitées ou incomplètes. En outre, les réseaux blockchain sont sujets à une sorte de violation de la sécurité connu sous le nom d'attaque 51%. Cette attaque implique une équipe de mineurs qui possèdent plus de 50% des blocs d'un réseau blockchain. Les mineurs obtiennent une autorité du réseau et pourraient empêcher toute nouvelle transaction en ne leur donnant pas leur consentement. Cinq cryptomonnaies ont récemment été victimes de cette attaque. En outre, un dossier patient peut contenir des données sensibles qui ne conviennent pas pour figurer dans la chaîne de blocs.

Problèmes d'interopérabilité

La blockchain souffre également du problème de l'interopérabilité, c'est-à-dire que les chaînes de blocs de divers fournisseurs et services de communication communiquent entre elles de manière transparente et appropriée. Ce défi crée des obstacles au partage efficace des données.

Défis de la normalisation

La technologie de la blockchain en est encore à ses balbutiements et elle sera donc certainement confrontée à des problèmes de standardisation en vue de son application pratique en médecine et en soins de santé. Un certain nombre de normes bien authentifiées et certifiées seraient exigées des autorités internationales de normalisation. Ces normes prédéfinies seraient utiles pour évaluer la taille, la nature des données et le format des informations échangées dans les applications blockchain. Ces normes examineront non seulement les données partagées, mais devront également servir de mesures de sécurité préventives.

Défis sociaux

La technologie des chaînes de blocs évolue toujours et fait donc face à des défis sociaux, tels que le changement de culture, en plus des défis techniques susmentionnés. Accepter et adopter une technologie complètement différente des méthodes de travail traditionnelles n'est jamais chose facile. Bien que l'industrie médicale s'achemine lentement vers la numérisation, il lui reste encore beaucoup à faire pour passer complètement à cette technologie, en particulier celle comme la blockchain, qui n'a pas encore été validée sur le plan clinique. Il faudra du temps et des efforts pour convaincre les médecins de passer de la paperasserie à la technologie. En raison de son faible taux d'adoption dans le secteur de la santé, la technologie et les politiques proposées sont relativement peu fiables. En raison de tous ces défis et menaces, nous ne pouvons pas, à ce jour, le qualifier de solution viable et universelle pour tous les problèmes de santé.

Conclusion

La technologie Blockchain est révolutionnaire. Elle va rendre la vie plus simple et plus sûre, en changeant la façon dont les informations personnelles sont stockées et dont les transactions de biens et de services sont effectuées.

Chapitre 3 Analyse et Conception

Introduction

La conception est l'étape principale dans le cycle de vie de création d'une application, elle a pour but de réaliser l'étude des données et les traitements à faire, elle aide également à réduire la complexité du système. C'est dans cette phase que s'appliquent les techniques de modélisation.

Dans ce chapitre, nous allons présenter les objectifs à atteindre de notre projet suivi d'une description générale de l'application, finalement nous allons présenter la modélisation de notre projet.

1. Description des besoins fonctionnels

1.1. Objectifs à atteindre

Notre travail doit accomplir certains buts. Ces buts peuvent être résumés dans ces points :

- Automatisation des tâches de gestion des documents du receveur.
- Signature des documents d'une façon automatique, rapide et plus facile.
- Vérification facile et rapide des documents.
- Attribution des documents à leurs propriétaires.

1.2. Description de l'application

L'application se compose de plusieurs espaces :

- **Index** : Contient une présentation de l'application et de tous les services présents.
- **Espace d'authentification** : L'utilisateur doit s'authentifier en utilisant un e-mail ou de son ID, et un mot de passe (Il doit faire l'inscription avant), ensuite il dispose d'un accès facile à ses informations selon son rôle :
    - **Espace Administrateur de l'application (Super Admin) :** Gestion de tous les paramètres de l'application, gestion des réseaux et la vérification des demandes d'accès reçues de la part des organismes afin d'être acceptés ou refusés.

- **Espace Administrateur du réseau (Network Admin)** : Gestion des organisations sur le réseau, affectation d'un admin à une organisation.
- **Espace Administrateur de l'organisme (Issuer) :** Gestion de son réseau en total, gestion des templates des documents, gestion des signataires, récepteurs et vérificateurs.
- **Espace Signataire (Signer) :** Reçoit les documents de la part de l'administrateur de l'organisme pour les signer.
- **Espace Récepteur (Recipient) :** Réception et visualisation de ses documents (signés et non signés)
- **Espace Vérificateur (Verifier) :** Vérification des documents, visualisation de son historique.

1.3. Fonctionnalités de l'application

Le tableau suivant résume les fonctionnalités principales de l'application :

Fonctionnalités	Description
Paramètres générales de l'application	
GENERALE	Paramètres généraux du site comme : les titres, descriptions..
THEME	Choisir le thème à appliquer à l'application
AIDE	Expliquer chaque élément de l'application
Gestion des utilisateurs : Super Administrateur (Super Admin)	
GESTION DES RESEAUX DE LA BLOCKCHAIN PRIVEE	Le super admin a pour but de gérer l'application, affecter les administrateurs pour chaque réseau
Gestion des utilisateurs : Administrateur du réseau (Network Admin)	
PROFIL	Le profil contient toutes les informations sur l'utilisateur actuellement authentifié
RECEPTION DES DEMANDES D'ACCES AU RESEAU	L'administrateur du réseau reçoit des demandes d'accès à son réseau et décide de les accepter ou rejeter
DESACTIVER UN ORGANISME	Il peut expulser un organisme de son réseau
LISTER LES ORGANISMES	Afficher une liste contenant les organismes appartenant au réseau actuellement.

Gestion des utilisateurs : Administrateur de l'organisme (Issuer)	
PROFIL	Le profil contient toutes les informations sur l'utilisateur actuellement authentifié
GESTION DES CERTIFICATS	L'administrateur de l'organisme gére les certificats en gérant les designs pour Chaque certificat
GESTION DES RECEPTEURS	L'administrateur de l'organisme gére les récepteurs en ajoutant, acceptant ou rejetant leurs demandes d'accès au réseau, affecter et signer des documents aux récepteurs..
GESTION DES SIGNATAIRES	L'administrateur de l'organisme gére les signataires en les ajoutant à son réseau et les affecter à des catégories des Certificats
GESTION DES VERIFICATEURS	L'administrateur de l'organisme gére les vérificateurs en leur donnant accès à son Réseau afin qu'ils vérifient les documents
CONTACT	
FORMULAIRE DE CONTACT	Formulaire disponible aux utilisateurs de L'applications afin de poser leurs questions
MESSAGERIE	
SERVICE DE MESSAGERIE	Les utilisateurs de l'application peuvent Échanger entre eux des messages
GESTION DES CERTIFICATS	
GESTION CERTIFICATS (Issuer)	L'administrateur de l'organisme peut Ajouter/modifier/supprimer un document
SIGNER CERTIFICATS (Issuer + Signer)	Chaque document doit être signé par les signataires affectés par l'organisme, et après cela l'issuer doit signer le certificats lui-même
CONSULTER CERTIFICATS (Issuer + Recipient)	- Chaque récepteur peut consulter ses propres documents (signés ou non signés) - Chaque organisme peut lister tous ses certificats

VERIFIER DOCUMENTS	- Chaque organisme peut vérifier les documents signés - Chaque vérificateur peut vérifier l'état d'un certificat à partir de son ID

Table 1 : Fonctionnalités de l'application

2. Modélisation UML

2.1. Acteurs et leurs rôles

Dans notre application, nous envisageons six acteurs qui sont :

Table 2 : Liste des acteurs et leurs rôles

Acteur	Rôle
Super Administrateur (Super Admin)	- Authentification - Gestion des réseaux - Gestion des paramètres de l'application
Administrateur du réseau (Network Admin)	- Authentification - Gestion des organismes - Affectation des admins aux organismes - Gestion du profile - Envoie et réception de messages
Administrateur de l'organisation (Issuer)	- Authentification - Gestion des récepteurs - Gestion des documents - Gestion des designs - Gestion des signataires - Gestion des vérificateurs - Gestion du profile - Envoie et récéption de messages
Récepteur (Recipient)	- Authentification - Demande d'ajout au réseau - Visualisation de ses documents - Gestion d'accès à ses documents - Gestion du profile - Envoie et réception de messages

Signataire (Signer)	- Authentification - Visualisation des documents affectés - Signer les documents - Gestion du profile - Envoie et réception de messages
Vérificateur (Verifier)	- Authentification - Demande d'ajout au réseau - Vérification des documents - Gestion du profile - Envoie et réception de messages

2.2. Diagrammes des cas d'utilisations

- **Utilisateur :** tous les acteurs héritent de l'acteur utilisateur

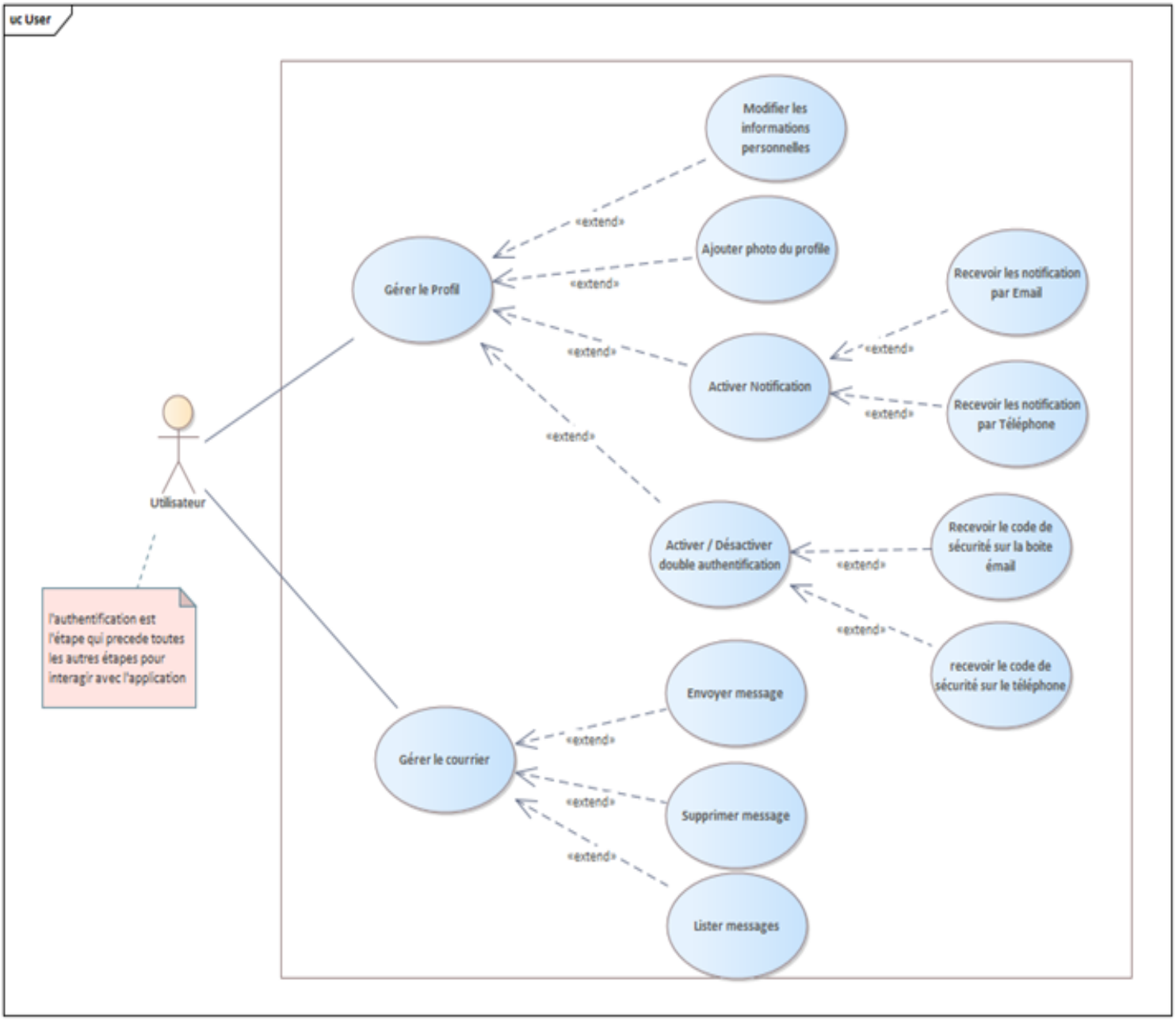


Figure 10 : cas d'utilisation de l'utilisateur

Administrateur du réseau (Network Admin) : C'est l'individu qui contrôle et gère tout son réseau.

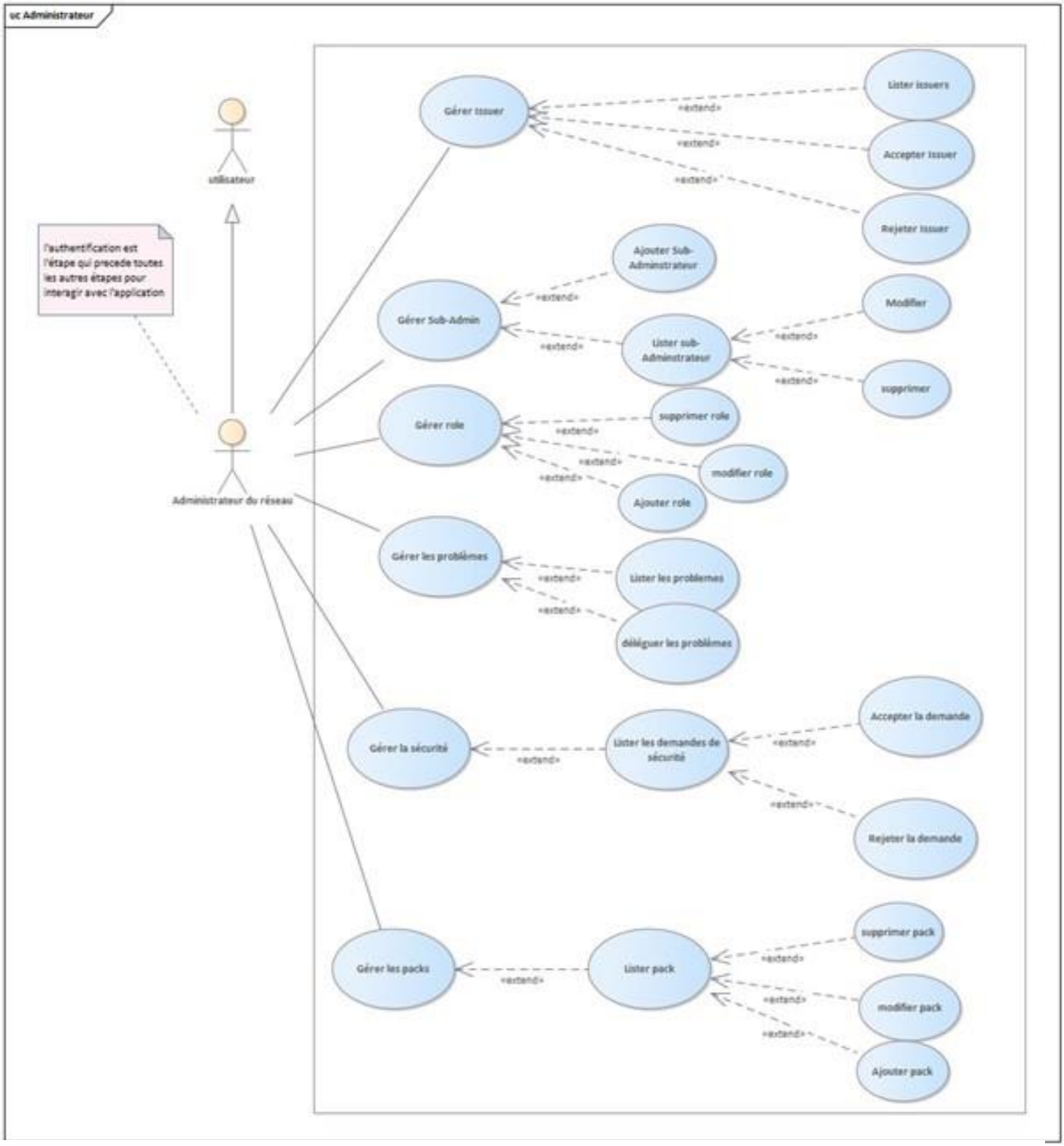


Figure 11:cas d'utilisation de l'administrateur

- **Administrateur de l'organisme (Issuer)** : C'est l'individu qui contrôle et gère son organisme.

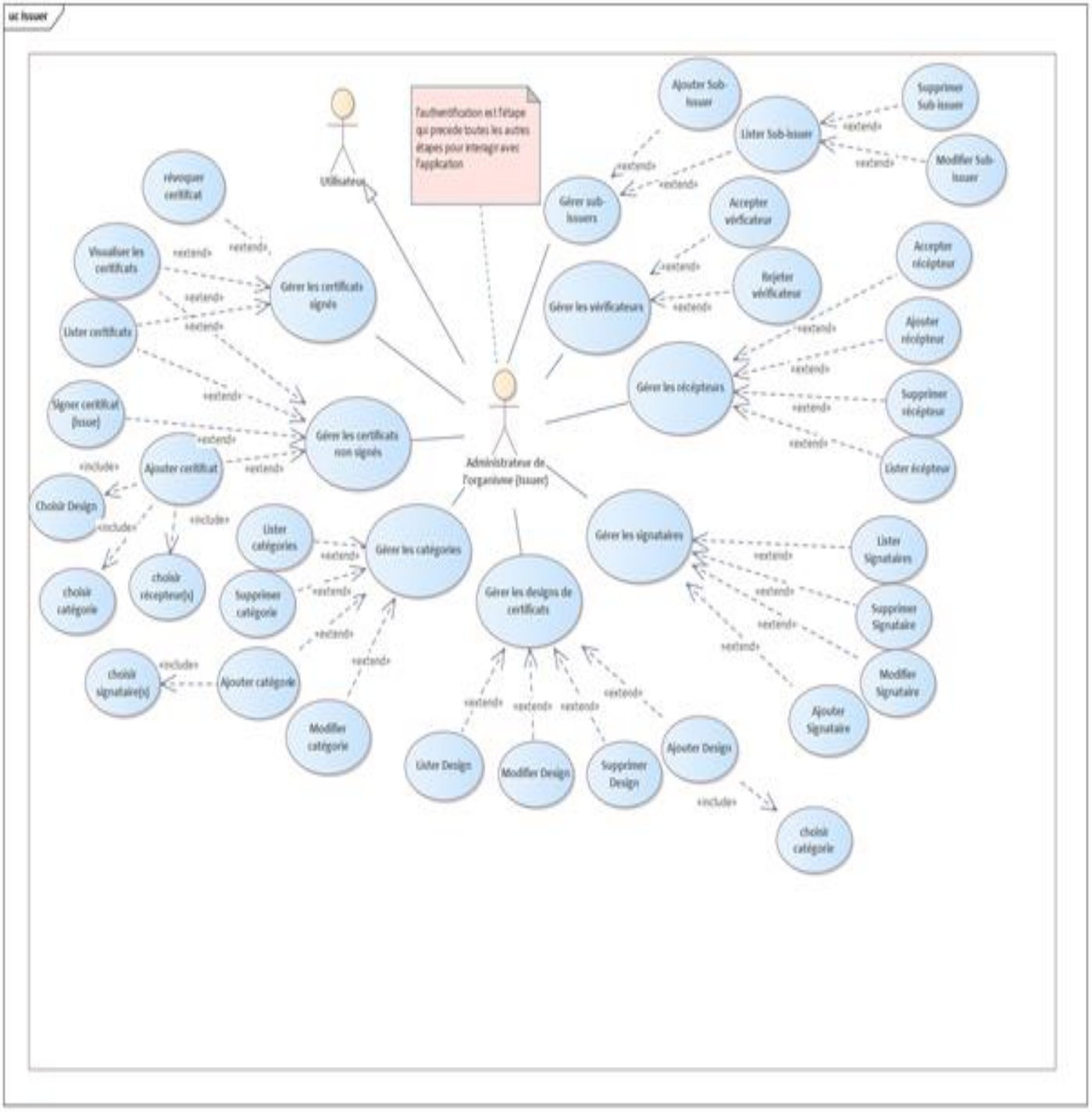


Figure 12: : cas d'utilisation Issuer

- **Récepteur (Recipient) :** C'est l'individu qui a un compte où il peut voir ses documents signés et non signés.

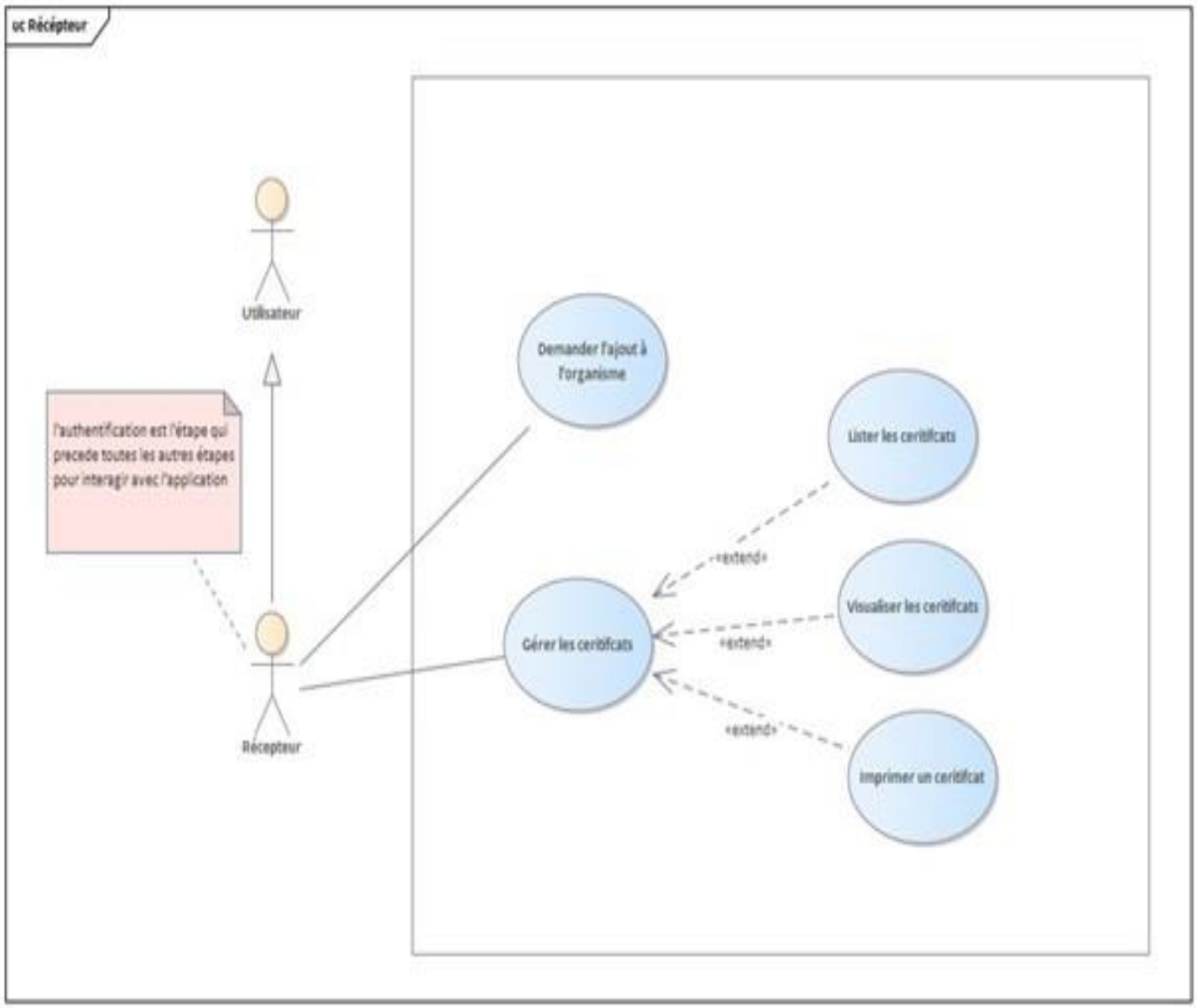


Figure 13: cas d'utilisation de Récepteur

- **Signataire (Signer)** : C'est l'acteur qui a était ajouté par l'administrateur de l'organisme pour signer les documents.

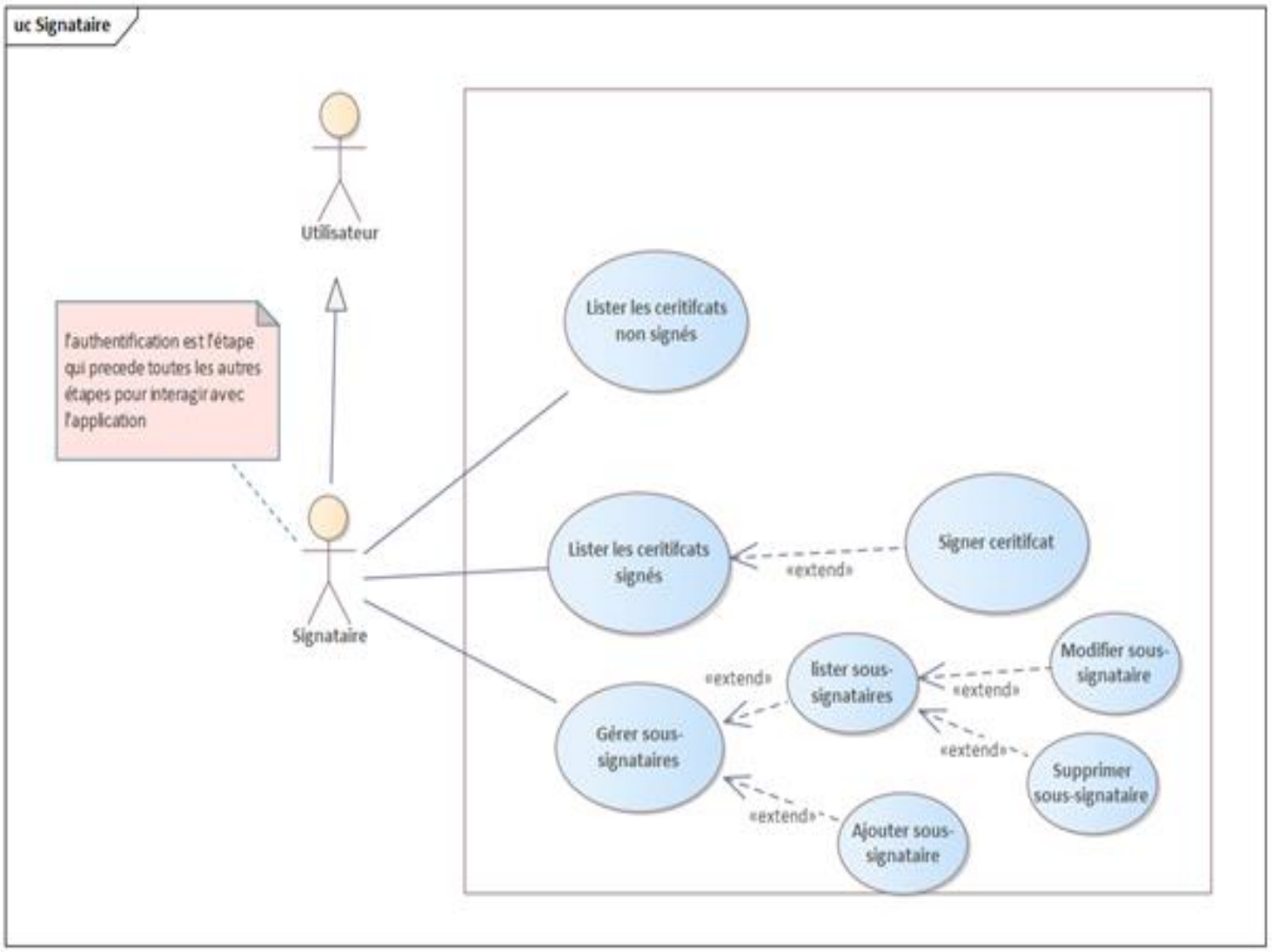


Figure 14: cas d'utilisation de signataire

- **Vérificateur (Verifier) :** C'est l'acteur qui rejoint le réseau pour vérifier les documents.

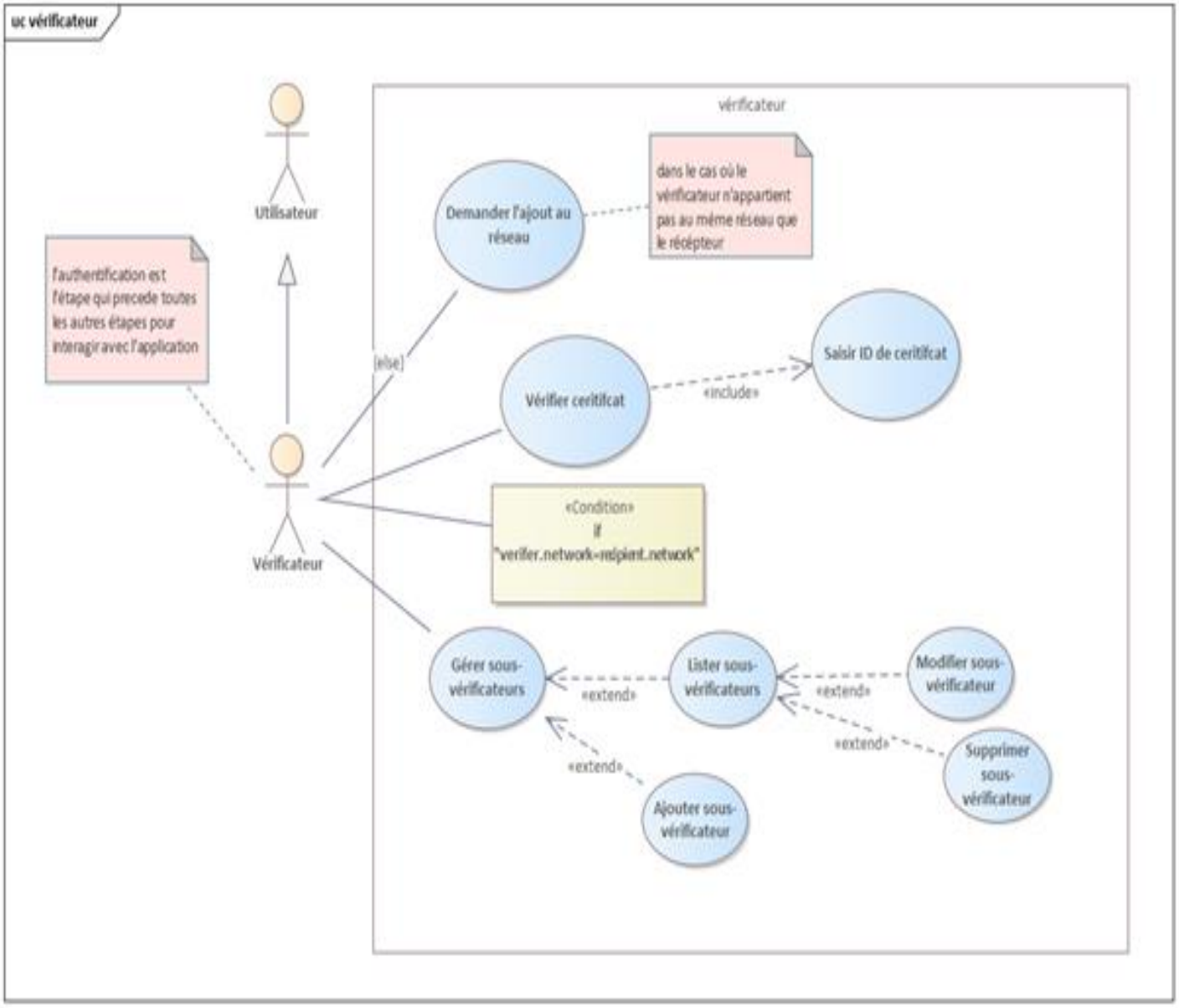


Figure 15: cas d'utilisation de vérificateur

2.3. Diagramme de séquences

Nous allons présenter certains diagrammes pour quelques cas d'utilisations pour chaque acteur :

- **Diagramme de séquence d'authentification pour tous les utilisateurs :**

La fonction s'authentifier permet à l'utilisateur de s'authentifier en utilisant son e- mail ou son ID et un mot de passe.

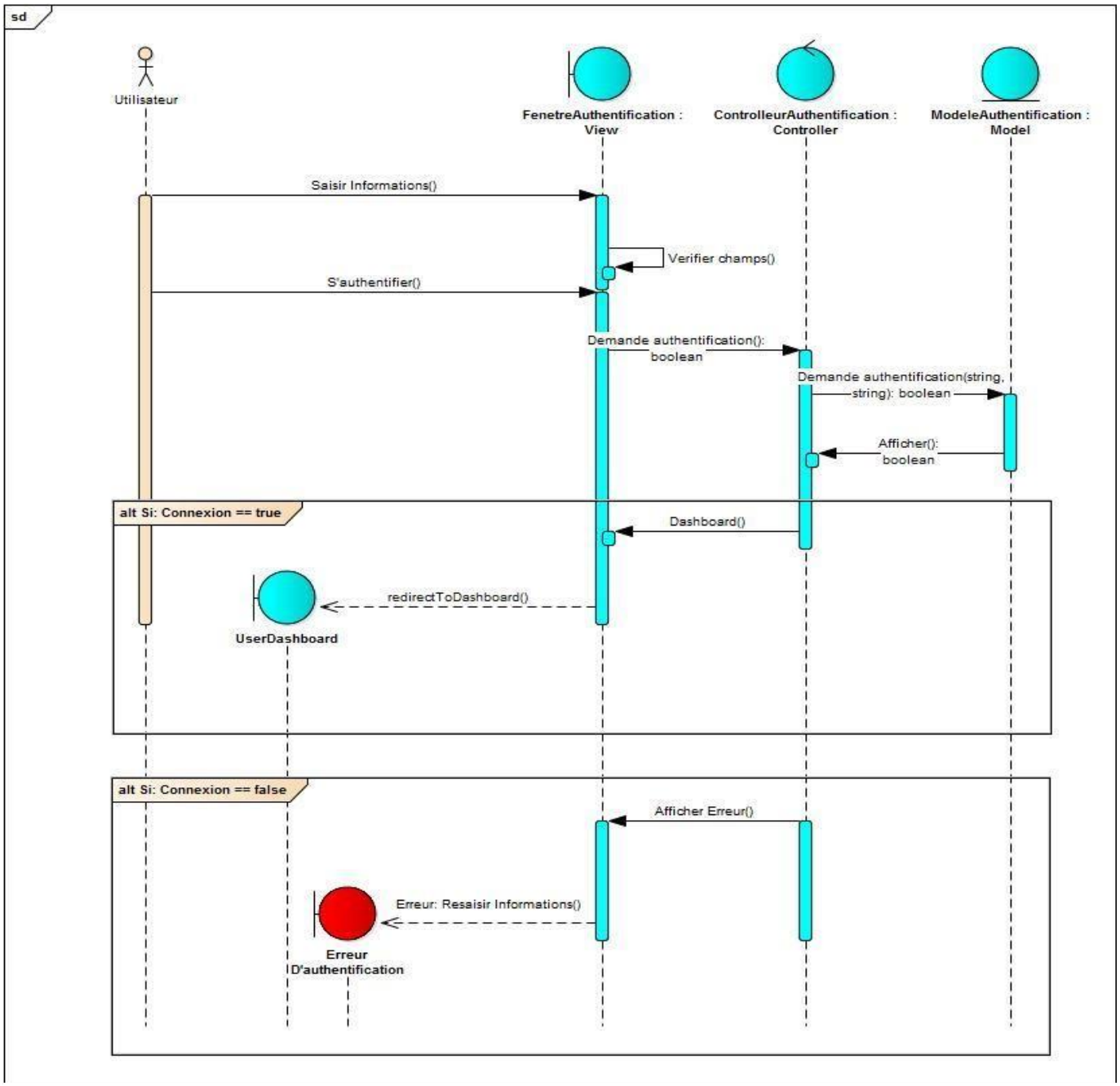


Figure 16: Diagramme de séquence d'Authentification

❖ **Diagramme de séquence de gestion d'organismes de l'Admin du réseau**

La fonction de gestion des organismes permet à l'administrateur du réseau d'approuver ou rejeter la demande d'ajout d'un organisme.

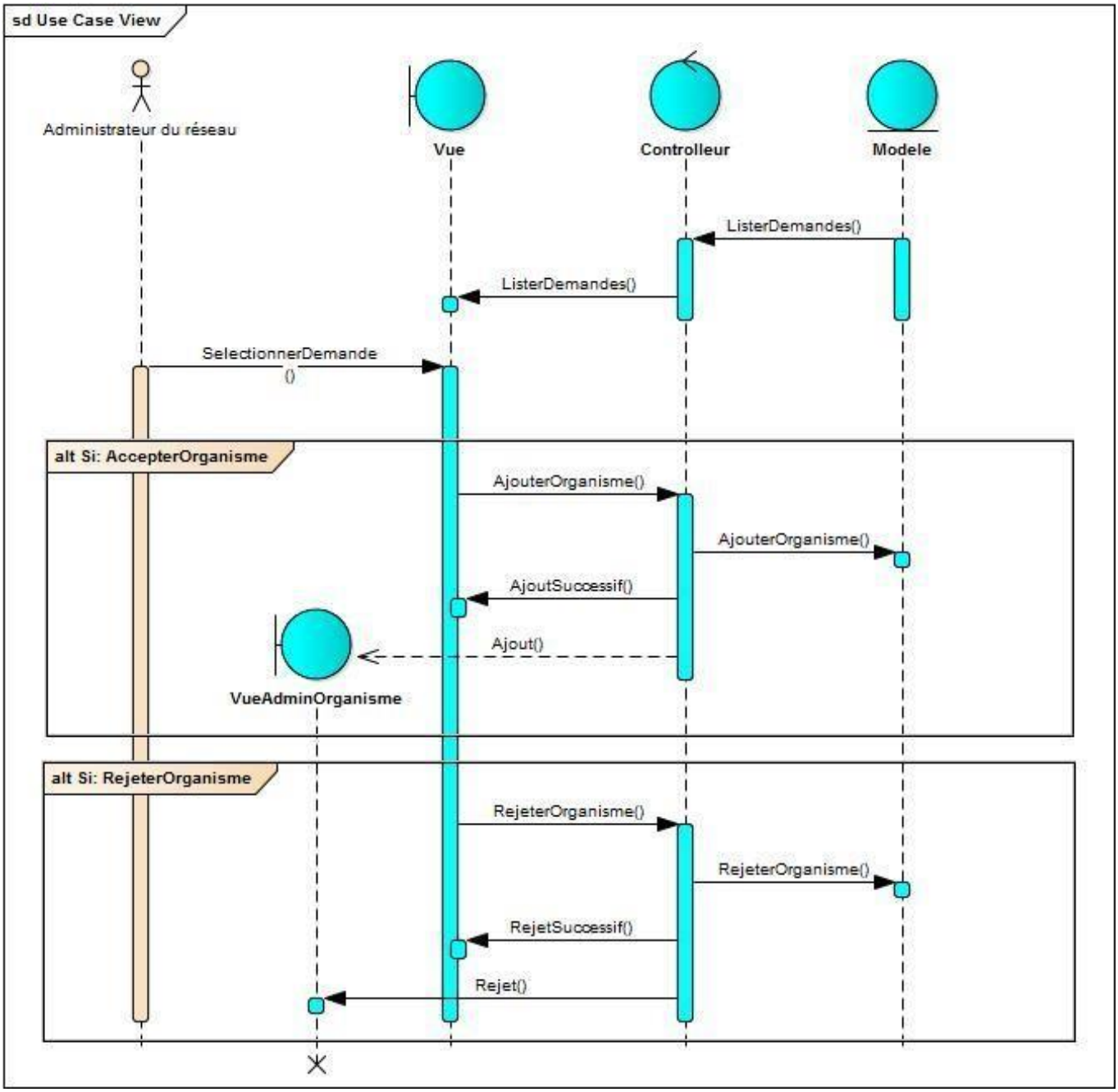


Figure 17 : Diagramme de séquence de Gestion des organismes

❖ **Diagramme de séquence d'ajout d'un document de l'Admin de l'organisme**

La fonction d'ajouter un document permet à l'admin de l'organisme d'ajouter un document pour un certain récepteur.

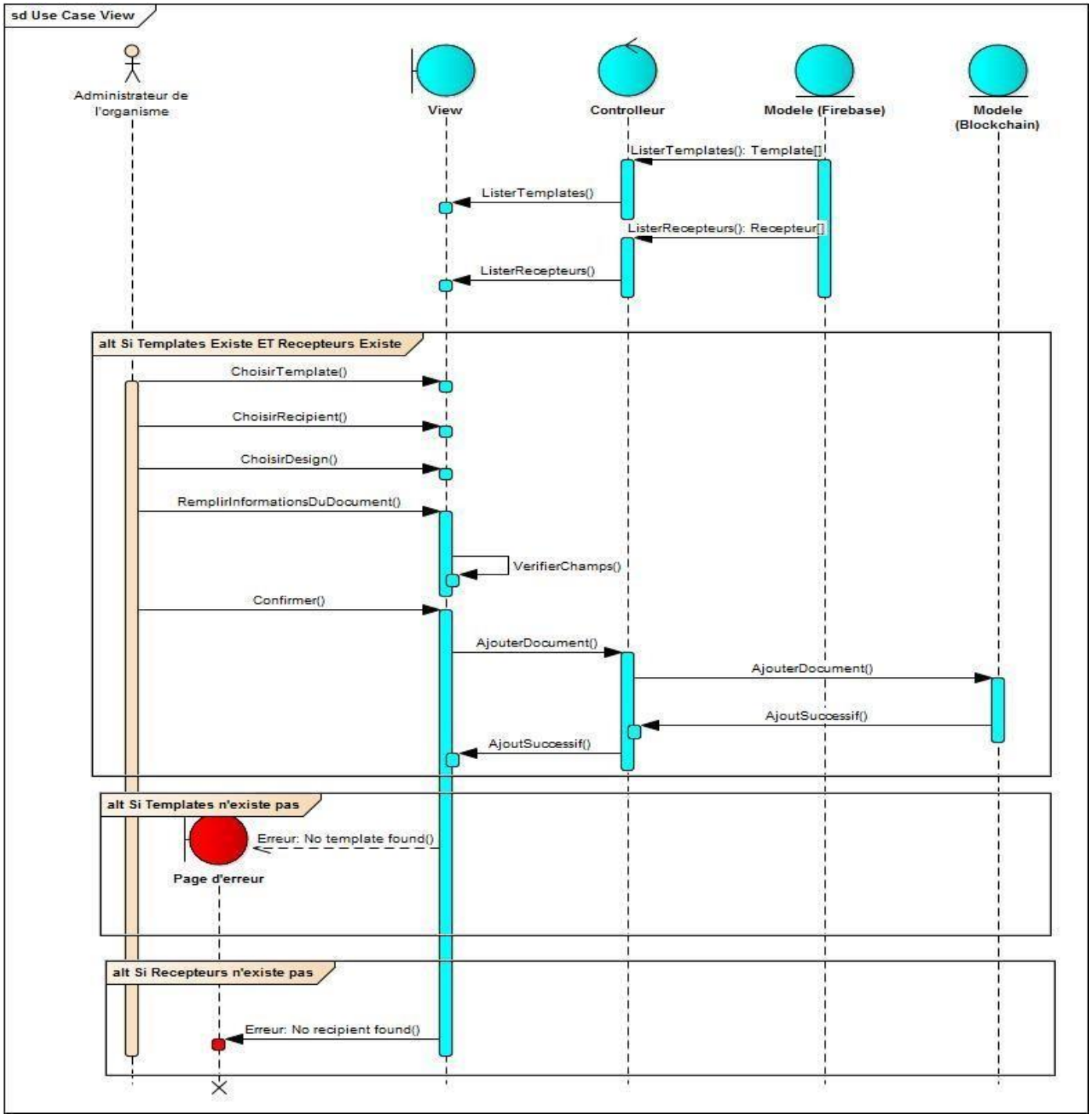


Figure 18 : Diagramme de séquence d'ajout d'un document

❖ **Diagramme de séquence de demande d'ajout du Récepteur**

La fonction de demande d'ajout permet au Récepteur de faire l'inscription et la demande de rejoindre un organisme.

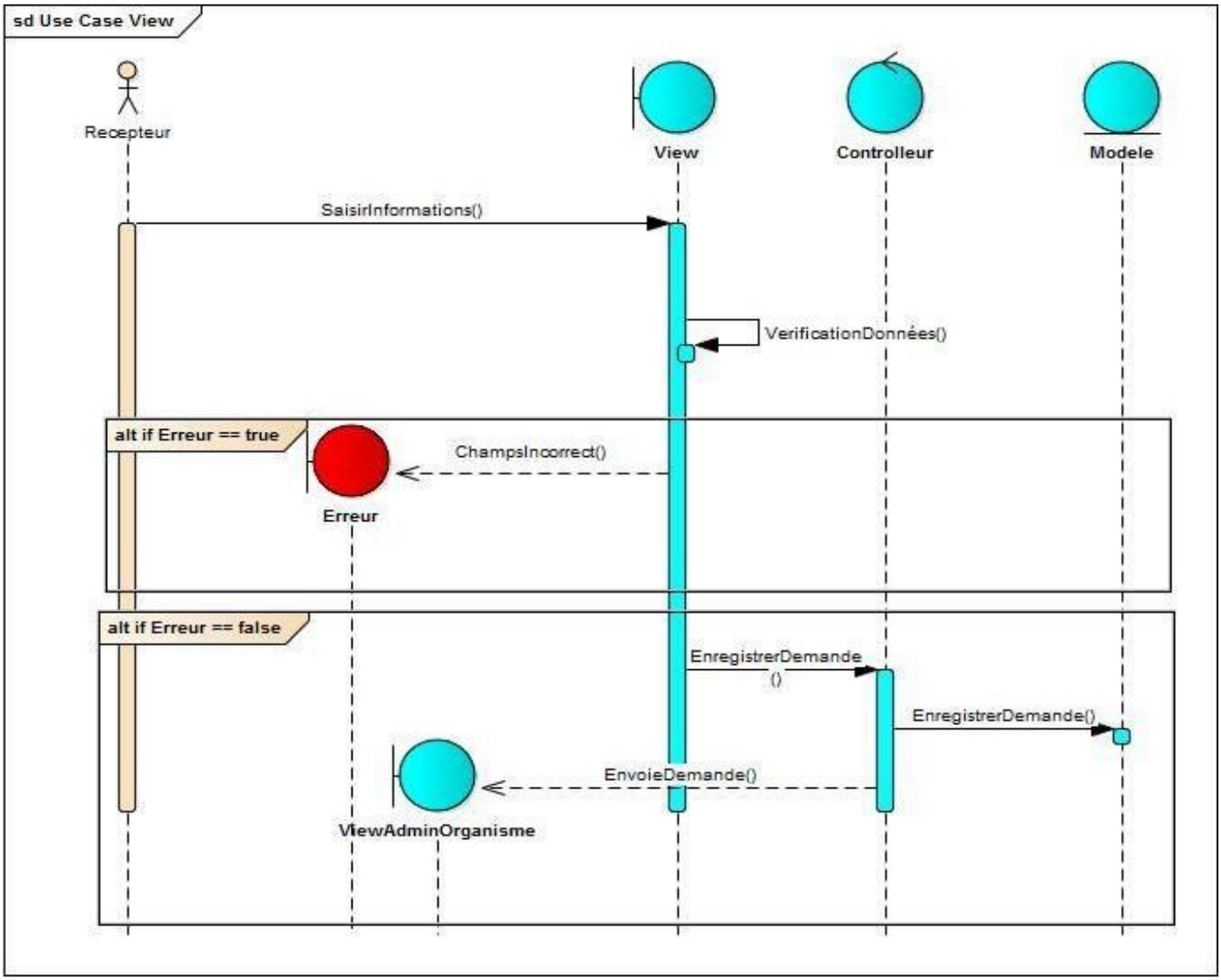


Figure 19 : Diagramme de séquence de demande d'ajout du Récepteur

❖ **<u>Diagramme de séquence de signature d'un document du Signataire</u>**

La fonction de signature permet le Signataire de signer un document

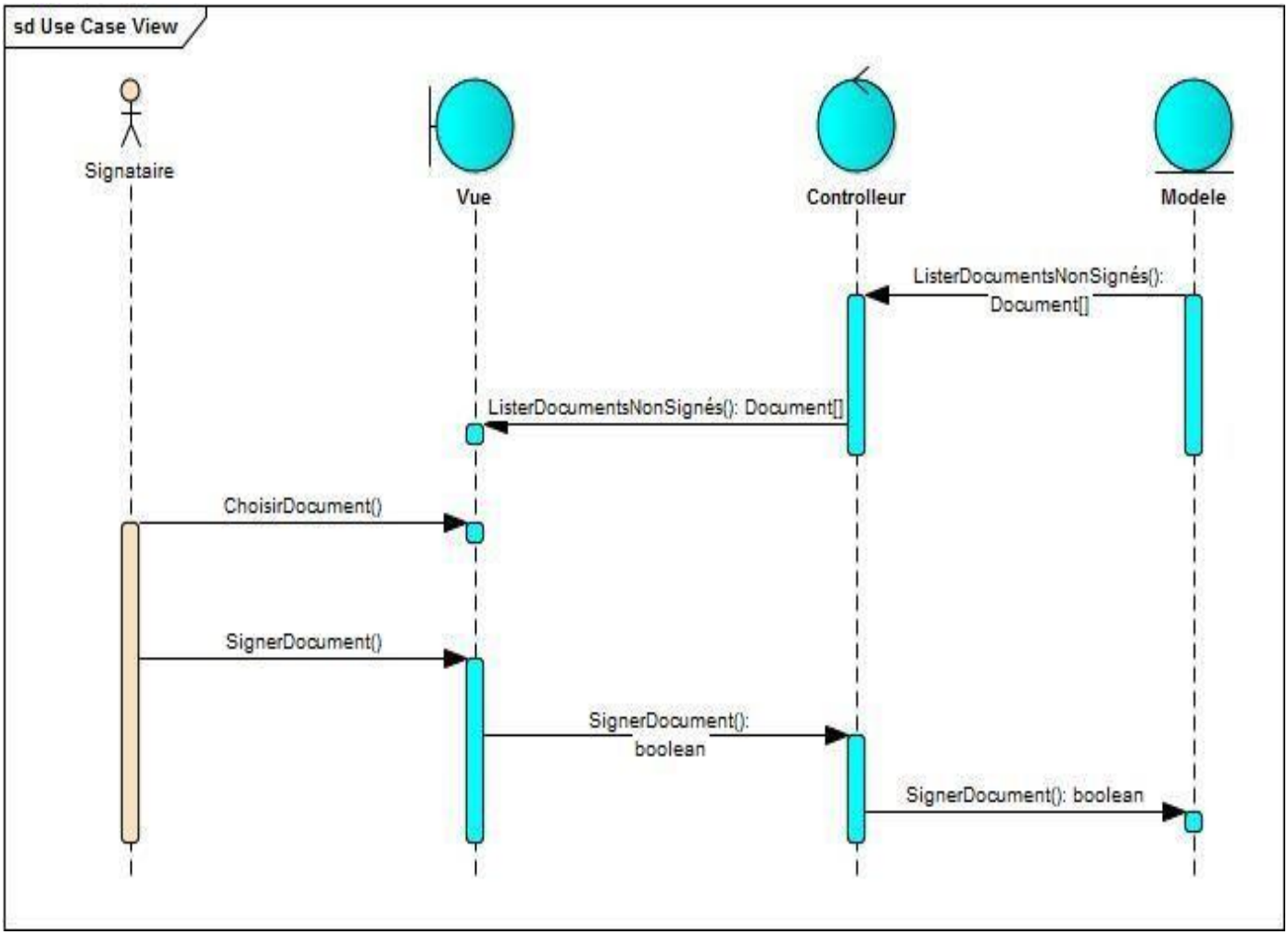


Figure 20 : Diagramme de séquence de signature d'un document du Signataire

❖ **Diagramme de séquence de vérification d'un document du Vérificateur**

La fonction de vérification de document permet au Vérificateur de vérifier les informations d'un document d'un Récepteur.

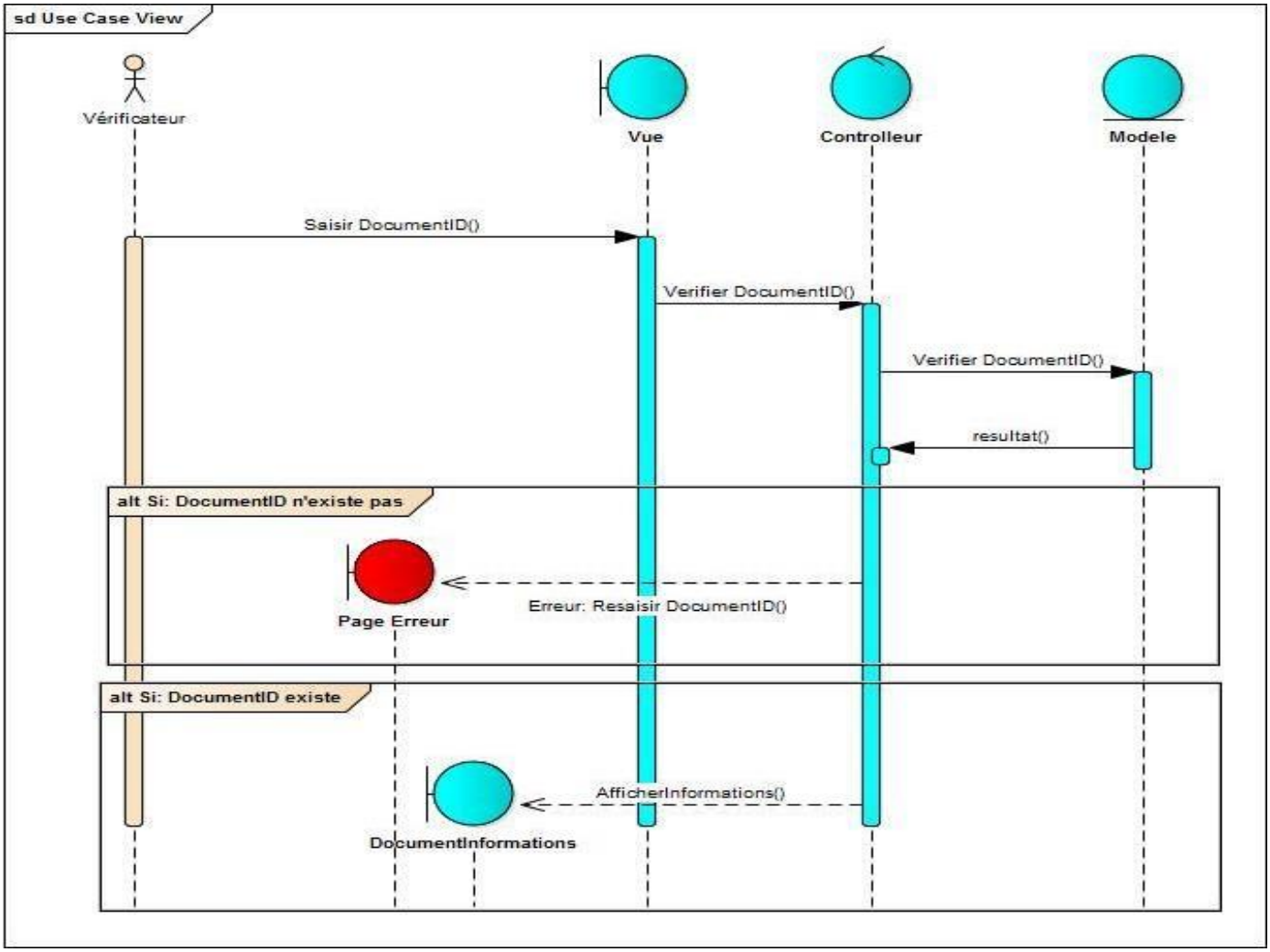


Figure 21 : Diagramme de séquence de vérification d'un document du Vérificateur

2.4. Diagramme de classes

Nous présentons notre diagramme de classe qui décrit les acteurs principaux ainsi que les différentes classes utilisées dans l'application et les relations entre eux.

On commence par la classe « Organisme » qui représente l'organisme utilisant l'application, Sidi Mohamed Ben Abdellah est un exemple d'organisme.

« OrganismGroup » est la classe qui hérite de « Organisme ». La faculté des Sciences et Techniques de Fès est un sous-groupe de l'université Sidi Mohamed ben Abdellah.

Les classes en relation avec les utilisateurs sont : « User », qui est la classe principale de laquelle hérite les autres utilisateurs, « Admin » est l'administrateur de l'organisme et fait le managment des « OrganismeGroup » dont « Issuer » est l'administrateur. Si « Organisme » contient un seul « OrganismeGroup » alors « Admin » peut être également « Issuer ».

Il y a également la classe « SubIssuer » qui est le subordonné de l'Issuer est auquel il délivre des tâches et de responsabilités. Le SubIssuer est donc manager par l'Issuer.

Toujours dans les classes utilisateurs il y a « Signer » qui signe les certificats et « SubSigner » qui est son subordonné, nous avons également la classe « Verifier » qui vérifie si les certificats sont signés par le Signer et pour ce il doit avoir l'accès de « Issuer », et la classe « SubVerifier» qui est son subordonné. Et enfin nous avons la classe « Recipient » qui représente le candidat qui reçoit les certificats.

Pour créer un certificat l'« Issuer » doit d'abord créer une catégorie qui appartient à la classe « Category » chaque certificat suit un design et pour que la création d'un certificat puisse être possible l'issuer doit acheter des « Pack ».

Nous avons également plusieurs interfaces :

- de gestion des subordonnés : « GestionSubAdmin », « GestionSubIssuer » ;
- de gestion de quelques utilisateurs : « GestionSigner », « GestionRecipient » ;
- « GestionCertificate » ;
- « GestionDesign ».

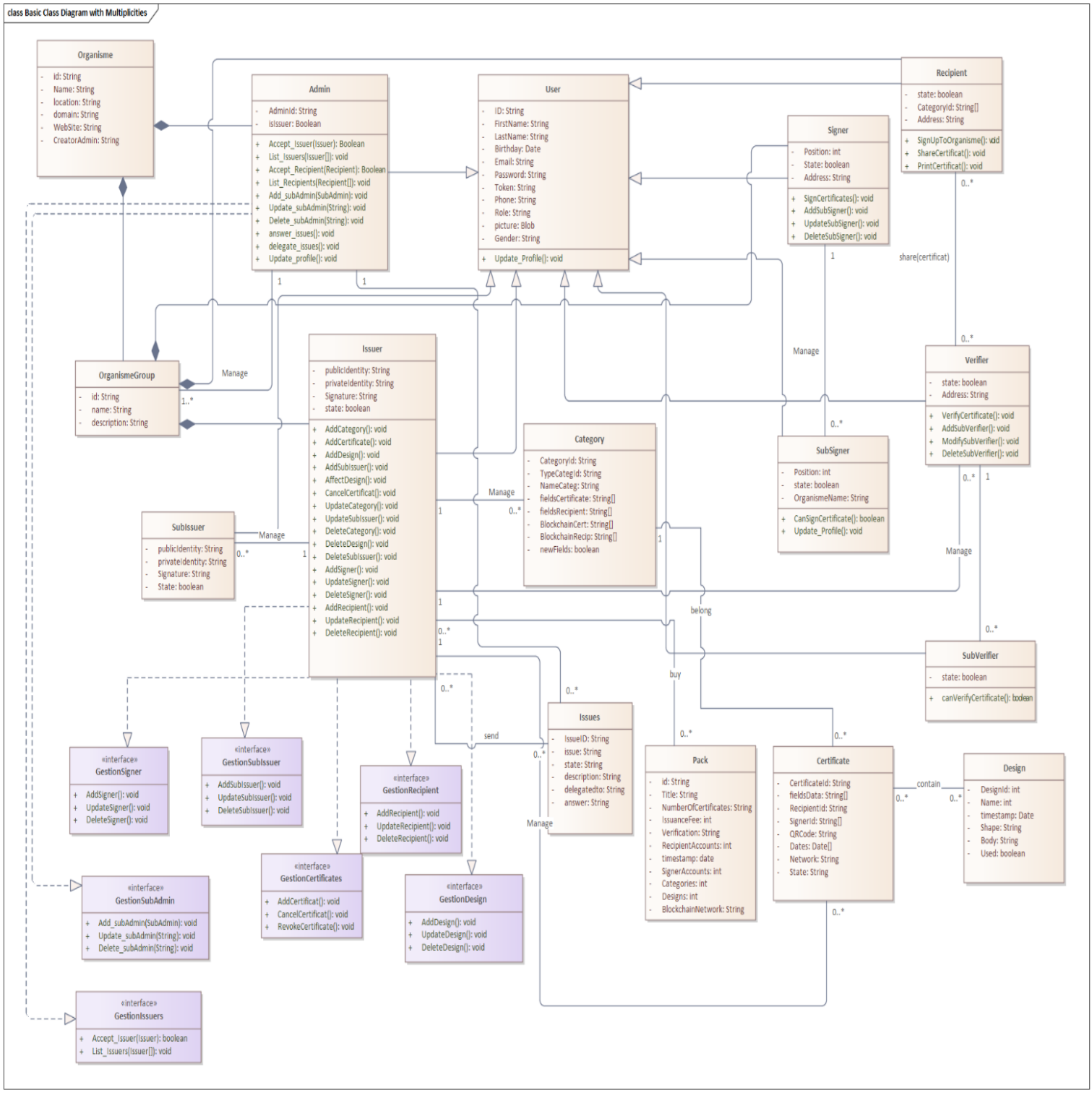


Figure 22 Diagramme de classes

Conclusion

Ce chapitre a été consacré au début à la description des différents objectifs du projet, description de l'application et ses fonctionnalités (cahier de charge), et ensuite nous avons abordé l'étude conceptuelle du système où nous avons présenté les diagrammes des cas d'utilisations, les diagrammes de séquences et le diagramme de classes. Dans le chapitre suivant nous allons passer à la phase de mise en œuvre de l'application.

Chapitre 4 Interface de l'application

Introduction

Dans ce chapitre, nous présenterons les outils utilisés lors de la réalisation du projet ainsi que les principales interfaces de l'application avec une description de chaque fonctionnalité de chaque utilisateur.

Nous avons travaillé sur deux versions sur ce projet la première avec angular et firebase et actuellement nous travaillons sur une deuxième version avec angular et spring boot, donc puisque la nouvelle version n'est pas encore terminée nous allons utiliser la version demo sur laquelle nous avons travaillé les deux premiers mois du stage pour expliquer le processus complet d'un organisme ''Huwawei'' qui va générer des certificats d'achèvement des cours à leurs récepeteur ''élèves'' et comment on peut vérifier cet certificat. Ensuite, nous vous montrerons quelques interfaces de la nouvelle version sur laquelle nous travaillons actuellement.

1. Les outils de développement

Les différents logiciels et langages de programmation utilisés pour développer cette application :

- Angular :

Angular est une plate-forme de développement, construite sur TypeScript. En tant que plate-forme, Angular comprend :

- Un framework basé sur des composants pour la création d'applications Web évolutives.
- Une collection de bibliothèques bien intégrées qui couvrent une grande variété de fonctionnalités, notamment le routage, la gestion des formulaires, la communication client-serveur, etc.
- Une suite d'outils de développement pour vous aider à développer, créer, tester et mettre à jour votre code [9].

❖ Spring Boot :

SpringBoot est un framework Java open source utilisé pour créer un microservice. Il est développé par Pivotal Team et est utilisé pour créer des applications de ressort autonomes et prêtes pour la production [10].

Spring Boot fournit une bonne plate-forme aux développeurs Java pour développer une application Spring autonome et de qualité production que vous pouvez simplement exécuter.

Pourquoi Spring Boot ?

nous avons choisi Spring Boot en raison des fonctionnalités et des avantages qu'il offre, comme indiqué ici

- ✓ Il fournit un moyen flexible de configurer les Java Beans, les configurations XML et les transactions de base de données.
- ✓ Il fournit un traitement par lots puissant et gère les points de terminaison REST. Dans Spring Boot, tout est configuré automatiquement, aucune configuration manuelle n'est nécessaire.
- ✓ Il offre une application de ressort basée sur des annotations Facilite la gestion des dépendances Il comprend un conteneur de servlet intégré.

❖ MongoDB :

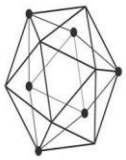
MongoDB est une base de données de documents, ce qui signifie qu'elle stocke les données dans des documents de type JSON. C'est la façon la plus naturelle de penser aux données, et qu'elle est beaucoup plus expressive et puissante que le modèle traditionnel de ligne/colonne.

Le modèle de document de MongoDB est simple à apprendre et à utiliser pour les développeurs, tout en offrant toutes les fonctionnalités nécessaires pour répondre aux exigences les plus complexes à n'importe quelle échelle. Il fournit des pilotes pour plus de 10 langues, et la communauté en a construit des dizaines d'autres.

- **Firebase :**

Firebase est un ensemble de services d'hébergement pour n'importe quel type d'application et il propose d'héberger en NoSQL et en temps réel des bases de données, du contenu de l'authentification sociale (Ex : Google, Facebook..), et des notifications, ou encore des services, tel que par exemple un serveur de communication temps réel. Ce service appartient aujourd'hui à de Google.

❖ Hyperledger :



HYPERLEDGER

Hyperledger est une blockchain privée open source soutenue par la Fondation Linux. Elle est la blockchain privée la plus complète du marché, mais elle est aussi une des plus complexes à déployer. Il s'agit d'une collaboration mondiale, regroupant des leaders des secteurs de la finance, de la banque, de l'Internet des objets, des chaînes d'approvisionnement, de la fabrication et de la technologie [11].

❖ **AWS (Amazon Web Services) :**

Amazon Web Services (AWS) est une division du groupe américain de commerce électronique Amazon.com, spécialisée dans les services de Cloud Computing, c'est la plate-forme cloud la plus complète et la plus largement adoptée au monde. Elle propose plus de 175 services complets issus de centres de données du monde entier. Des millions de clients dont certaines des startups les plus dynamiques au monde, de très grandes entreprises et des agences fédérales de premier plan utilisent AWS pour réduire leurs coûts, gagner en agilité et innover plus rapidement [12].

❖ Twilio API :

Twilio est une plateforme de développement pour les communications :

La plateforme d'engagement client Twilio.

Les interfaces de programme d'application (API) programmables de Twilio sont un ensemble de blocs de construction que les développeurs peuvent utiliser pour créer les expériences client exactes qu'ils souhaitent.

La plateforme d'engagement client Twilio peut être utilisée pour créer pratiquement n'importe quelle expérience numérique, en utilisant des fonctionnalités telles que SMS, WhatsApp, voix, vidéo, e-mail et même IoT, tout au long du parcours client. Twilio alimente les communications de plus de 190 000 entreprises et permet près de 932 milliards d'interactions humaines chaque année [13].

❖ **Metronic :**

Metronic est une Template HTML, CSS, JavaScript qui est utilisée pour construire les interfaces utilisateurs, elle est entièrement réactive et adaptée aux mobiles. Elle peut être utilisée pour tout type d'application web, y compris les panneaux d'administration personnalisés, les tableaux de bord d'administration, les backends des sites e-commerce… [14].

- GrapesJS :

Nous avons utilisé cette API juste pour le modèle de design v2.

GrapesJS est un framework de création de sites Web open source et polyvalent qui combine différents outils et fonctionnalités dans le d'aider les utilisateurs de votre application à créer des modèles HTML sans aucune connaissance du codage. C'est une solution parfaite pour remplacer les éditeurs WYSIWYG courants, qui sont bons pour l'édition de contenu mais inappropriés pour créer des structures HTML. Vous pouvez le voir en action avec les démos officielles, mais en utilisant son API, vous pouvez créer vos propres éditeurs [15].

2. Les interfaces de l'application

Nous allons maintenant présenter les différentes interfaces de l'application.

2.1. Inscription

Chaque utilisateur doit réaliser son inscription sur le site en remplissant certaines informations

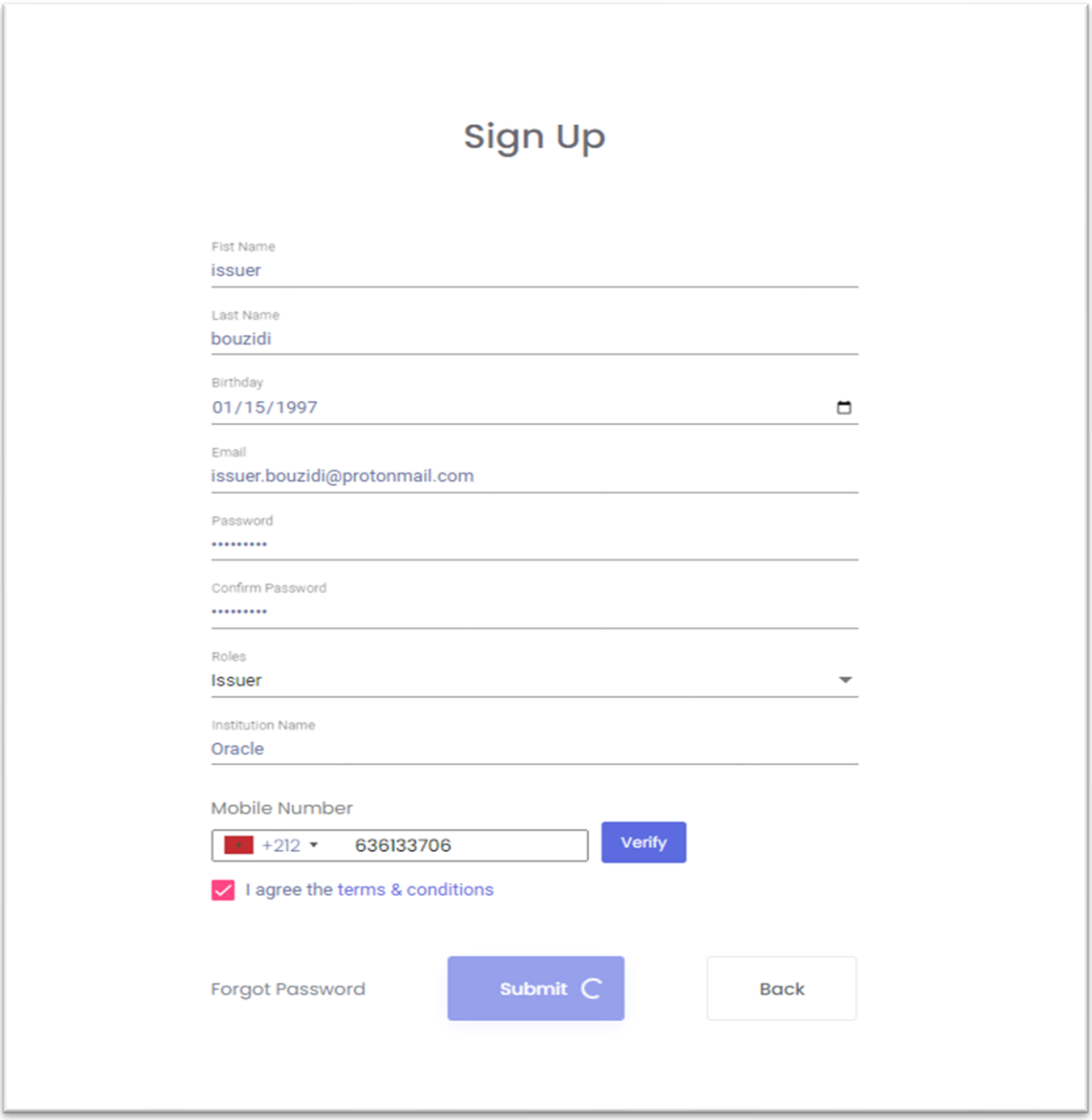
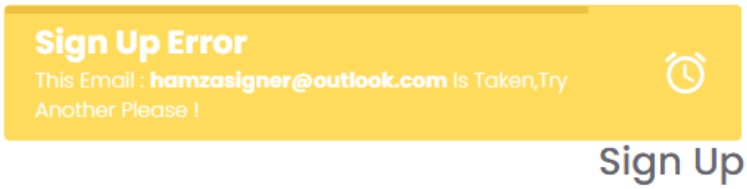


Figure 23:Interface de l'inscription d'un utilisateur

Au cas où l'email entré existe déjà :



2.2. Authentification

Chaque utilisateur doit s'authentifier, et selon son rôle il va être renvoyé vers son espace approprié (Il y a une vérification des identifiants du compte, si le compte n'existe pas ou n'est pas encore activé ou si un des identifiants est erroné le système affiche un message d'erreur).

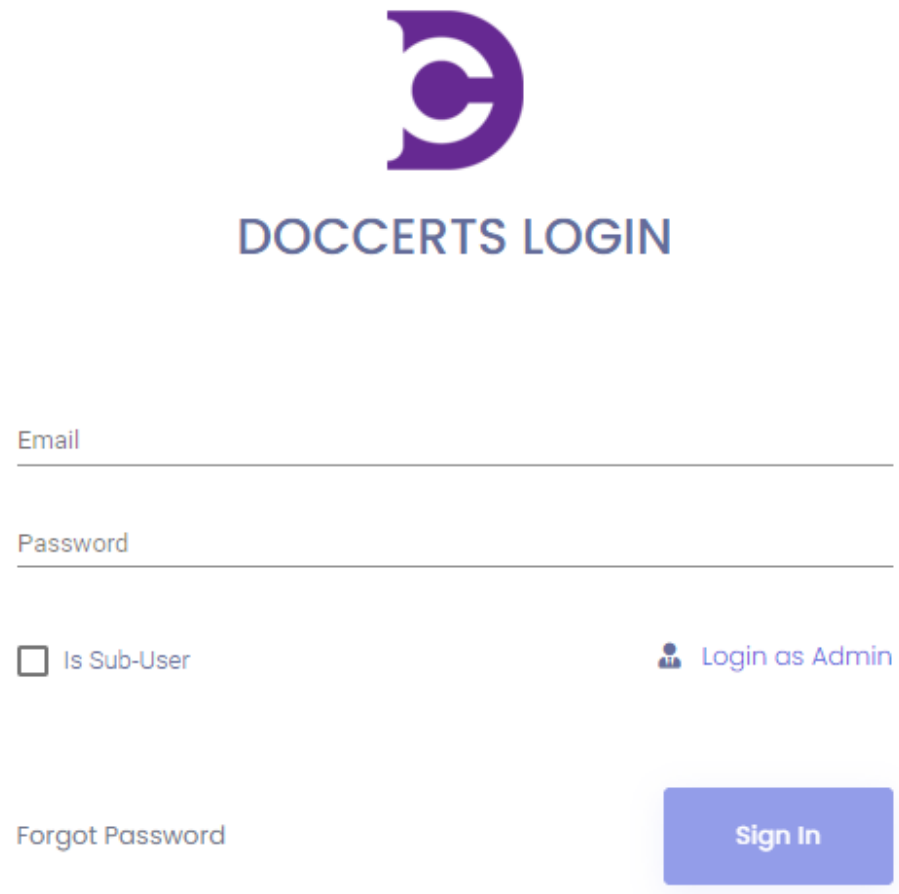


Figure 25:Interface d'authentification

Au cas où le compte de l'utilisateur est désactivé :

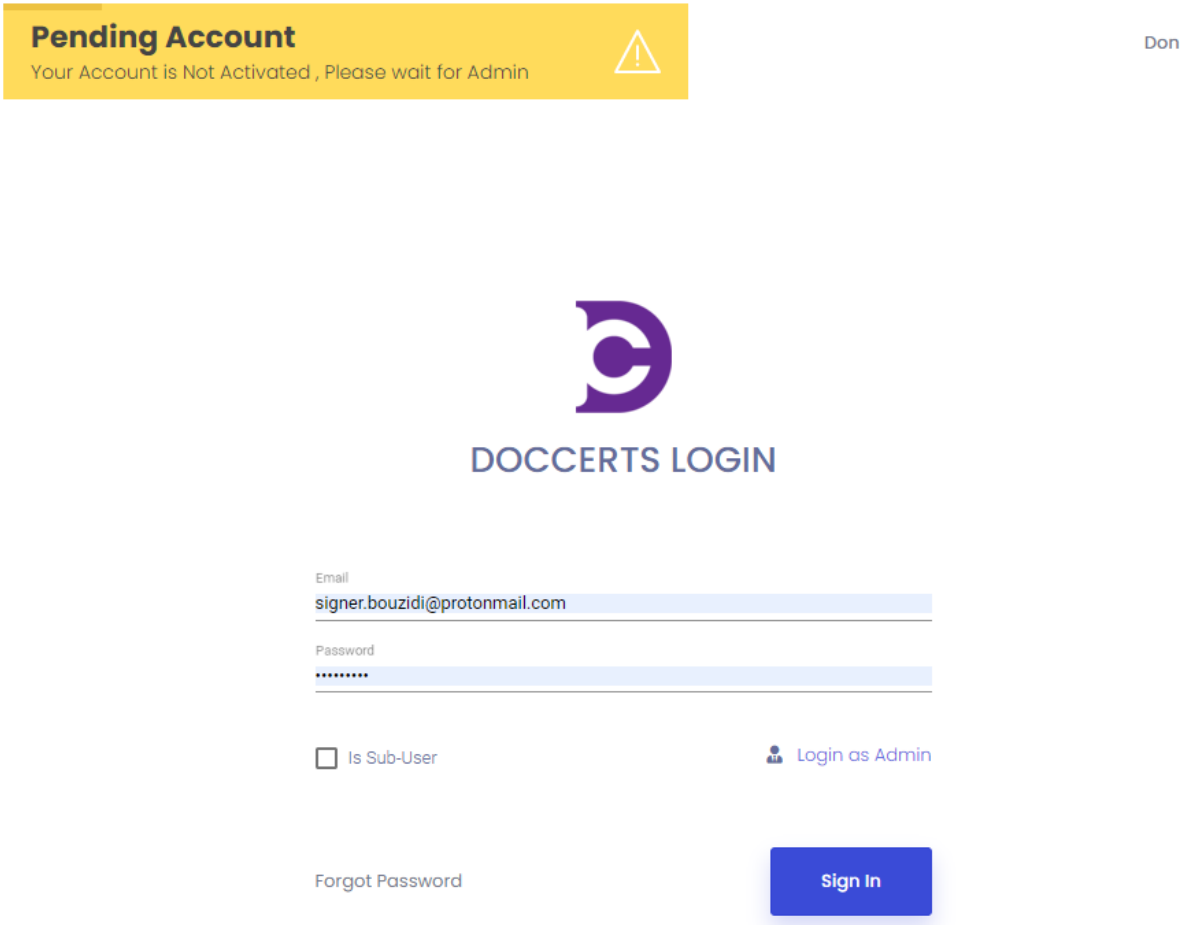


Figure 26:Interface d'authentification (cas du compte désactivé)

2.3. Profil de l'utilisateur

L'utilisateur a accès à son profil où il peut voir ses informations personnelles, et aussi peut les modifier.

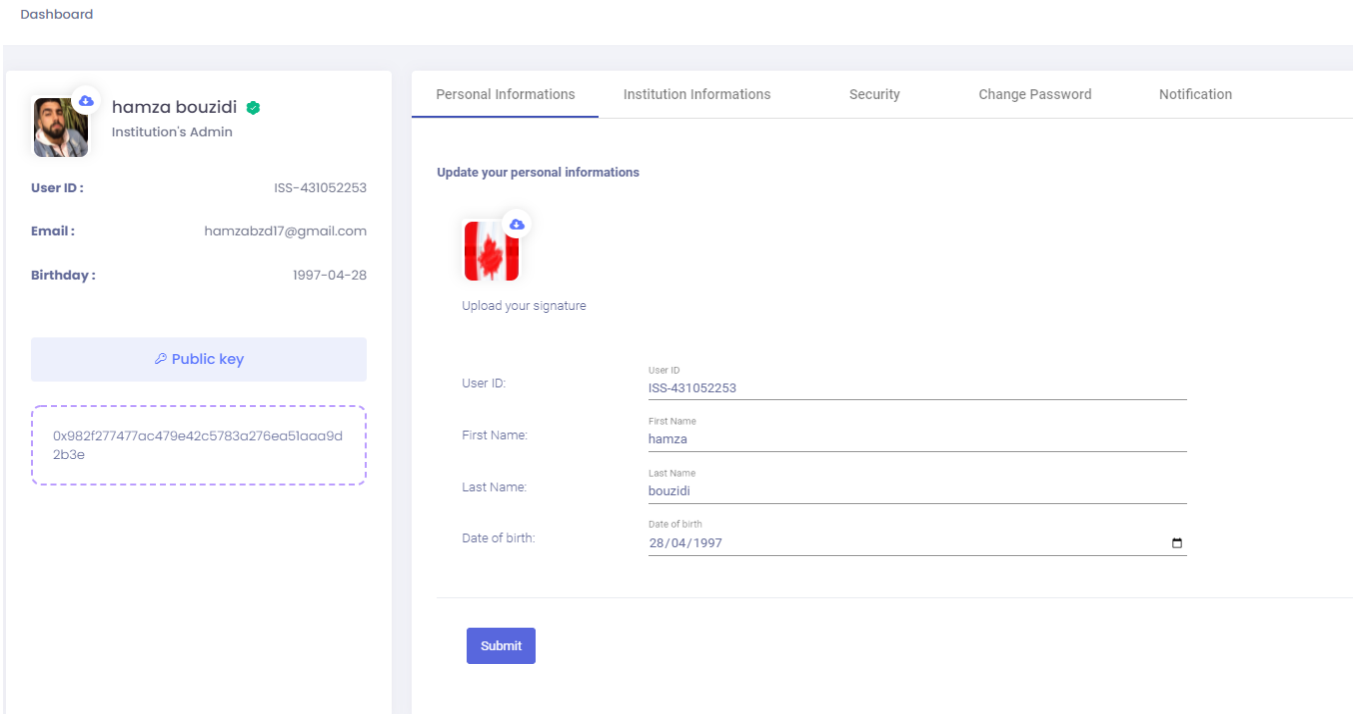


Figure 27 : Interface des informations personnelles de l'utilisateur

Par exemple dans cette figure, l'utilisateur peut voir son nom, prénom, date de naissance, adresse, numéro de téléphone, e-mail et sa photo de profil, et il peut les modifier.

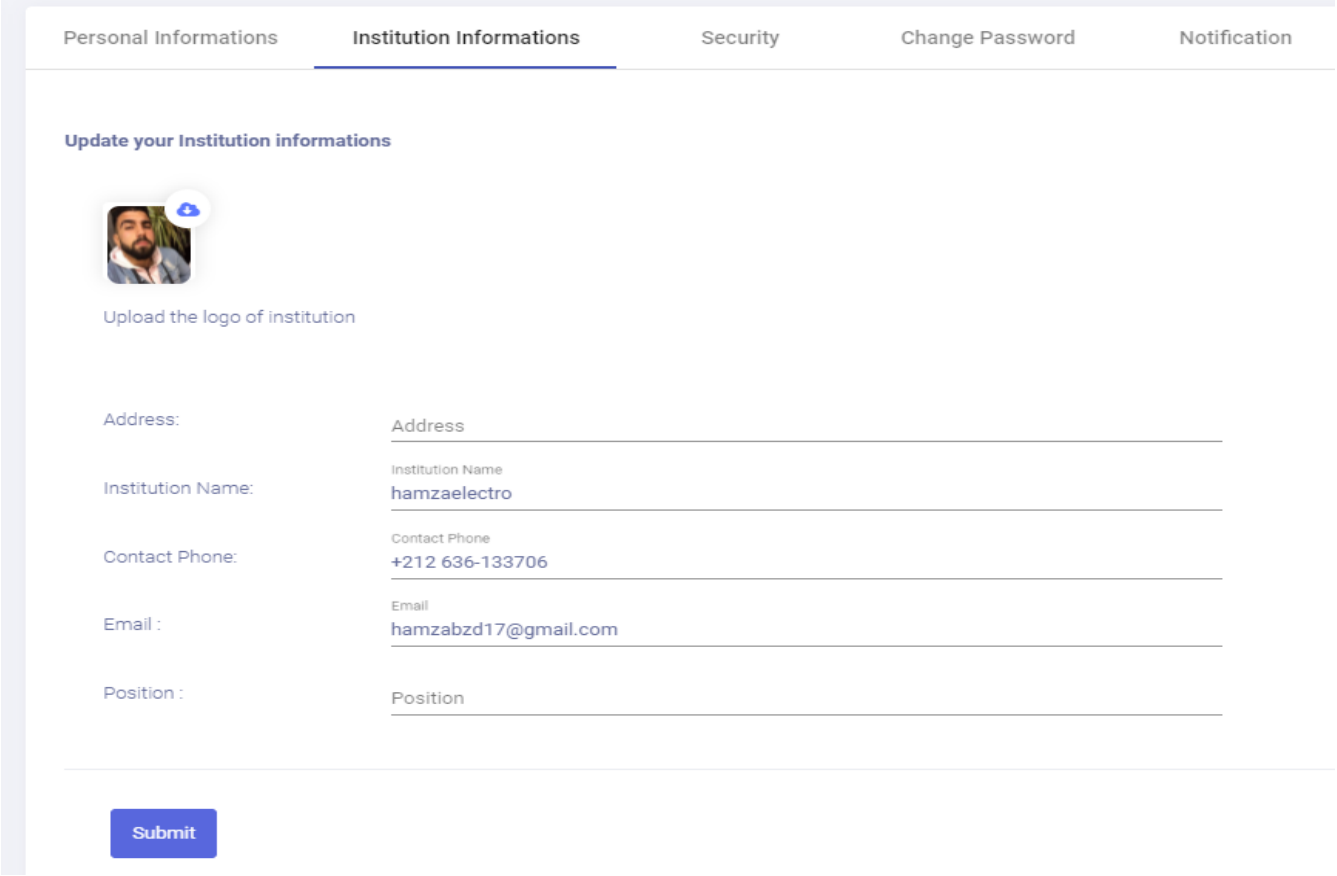


Figure 28: : Interface des informations d'institution

2.3.1. **Notification**

L'utilisateur peut choisir où recevoir les notifications e-mail , téléphone ou bien les deux :

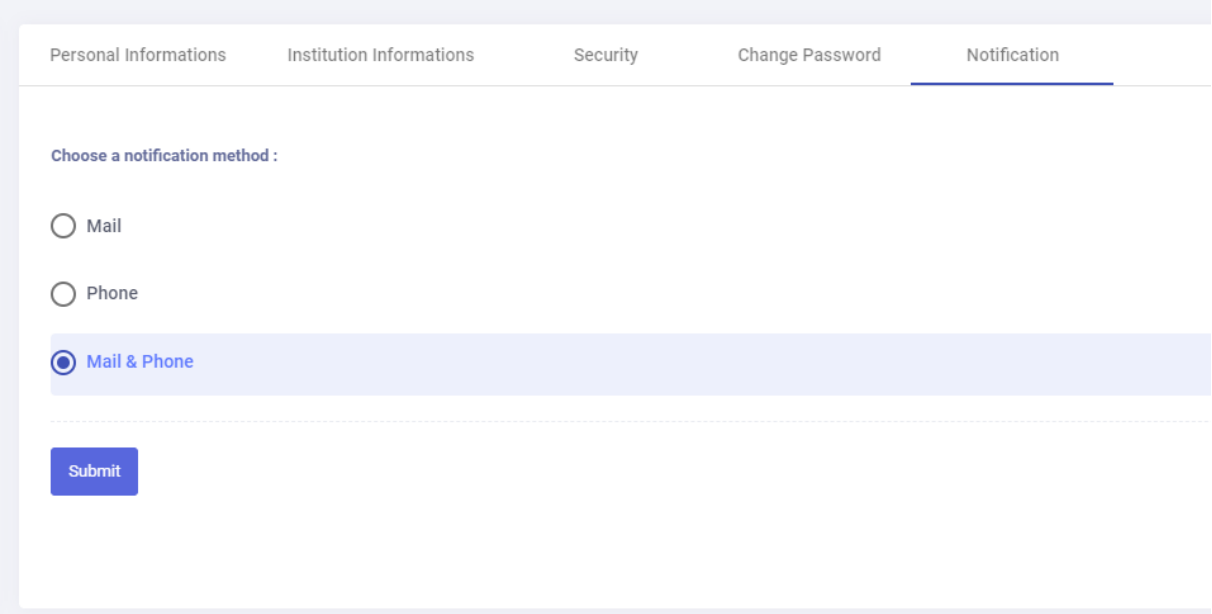


Figure 29: interface d'activation de la notification

2.4. Double authentification

L'utilisateur peut activer ou désactiver la double authentification.

Il peut choisir de recevoir le code sur son téléphone ou par e-mail ou les deux.

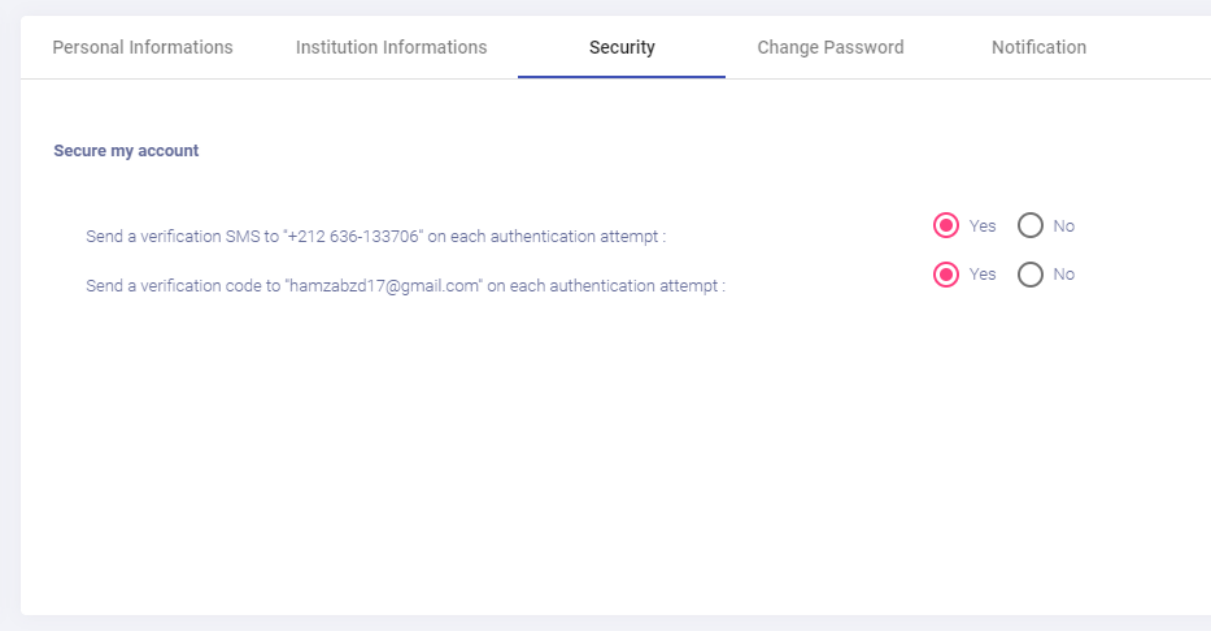


Figure 30: interface d'activation de la double authentification

Authentification Après avoir activé la double authentification mail & phone :

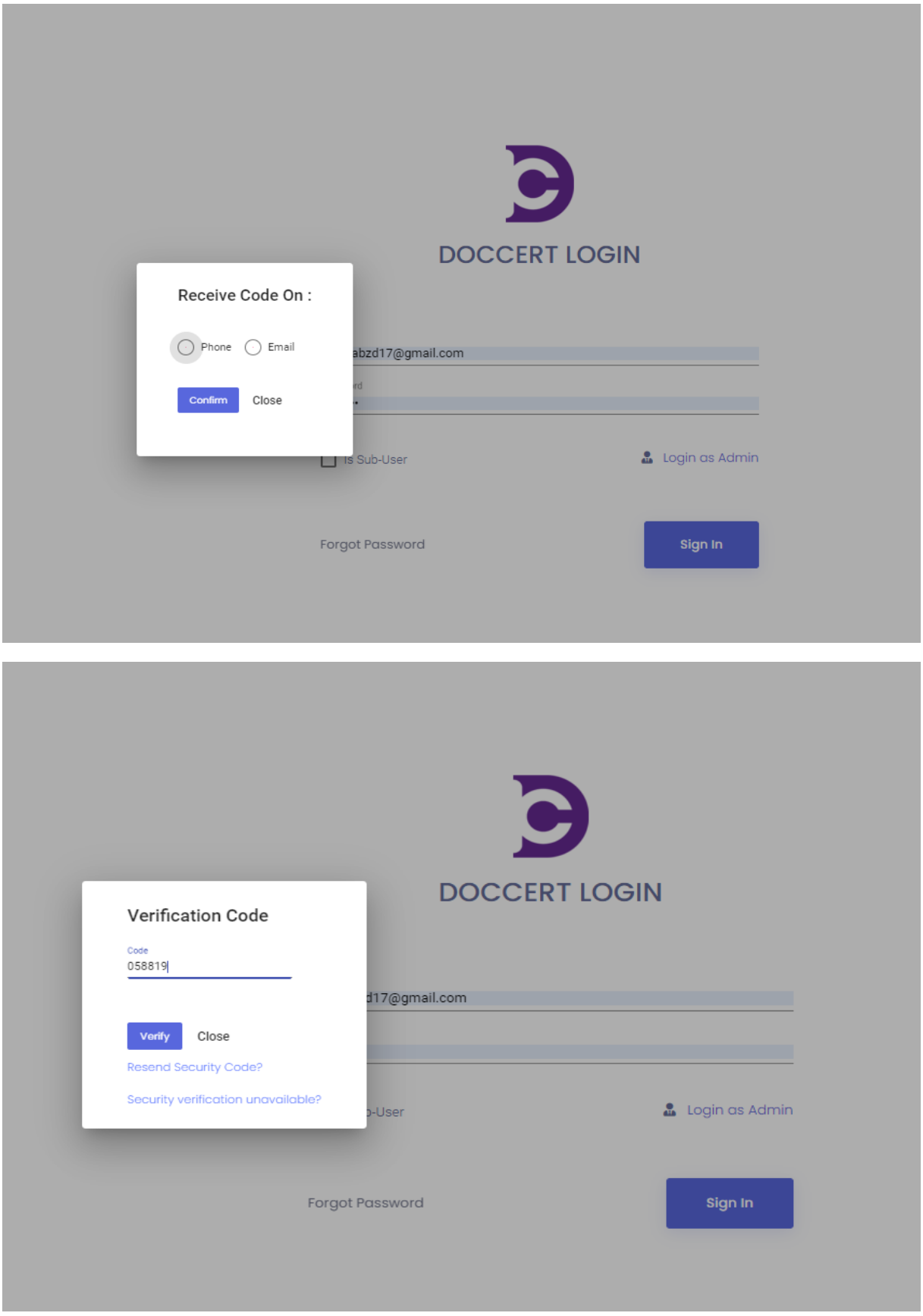


Figure 31: interface du code de vérification

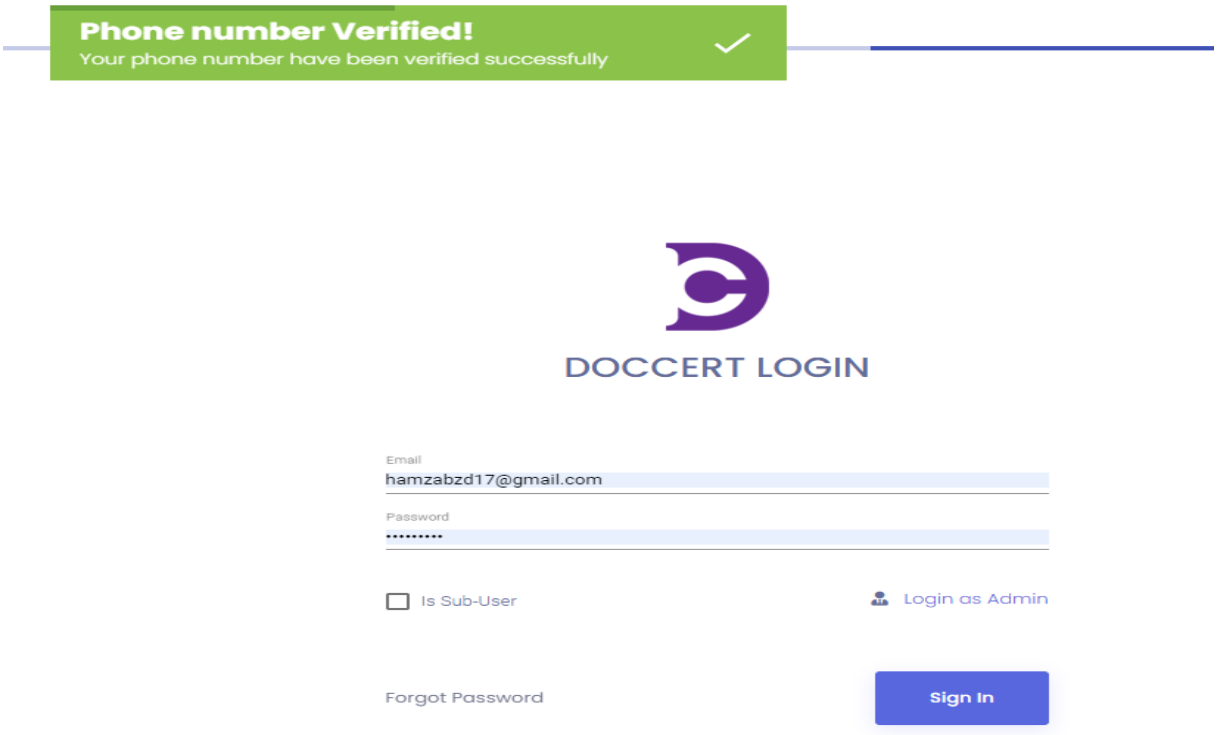


Figure 32 : interface réussite de l'authentification

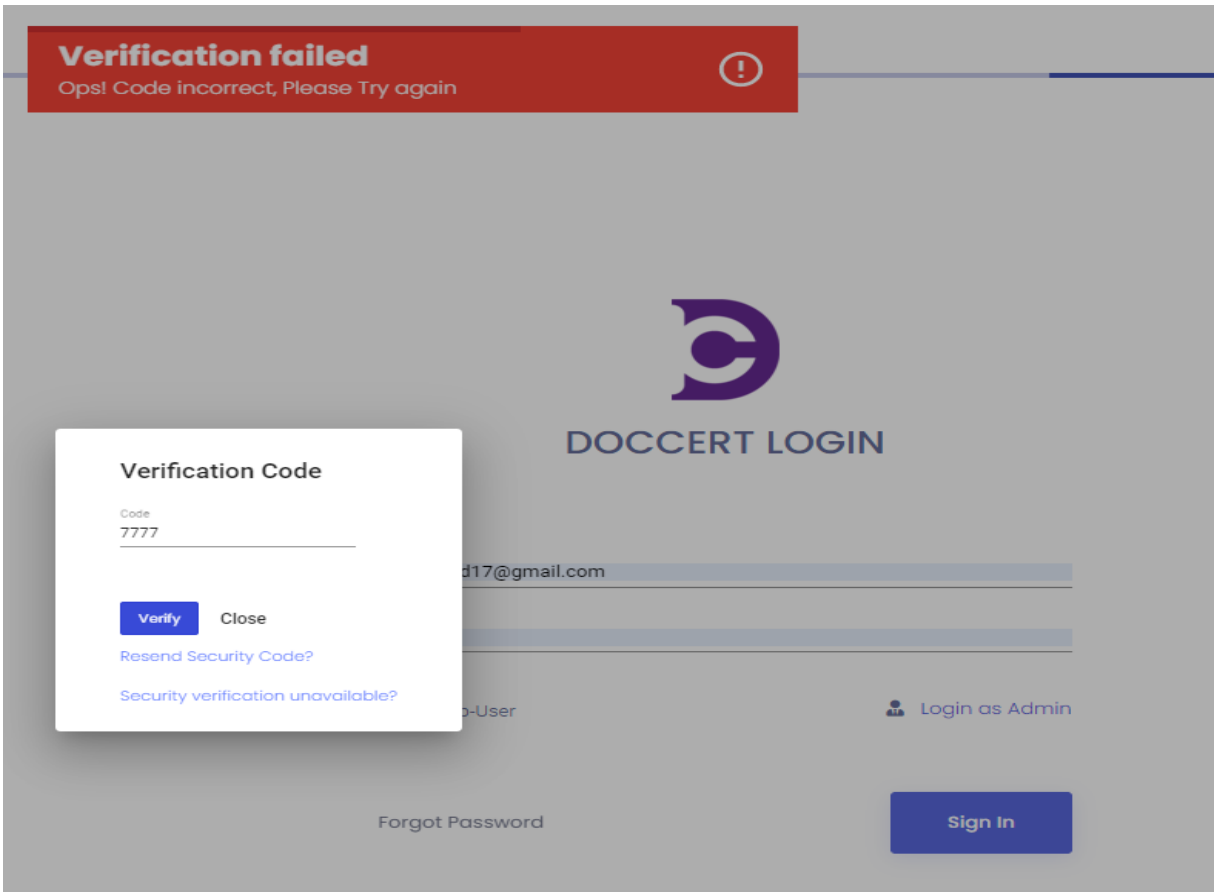
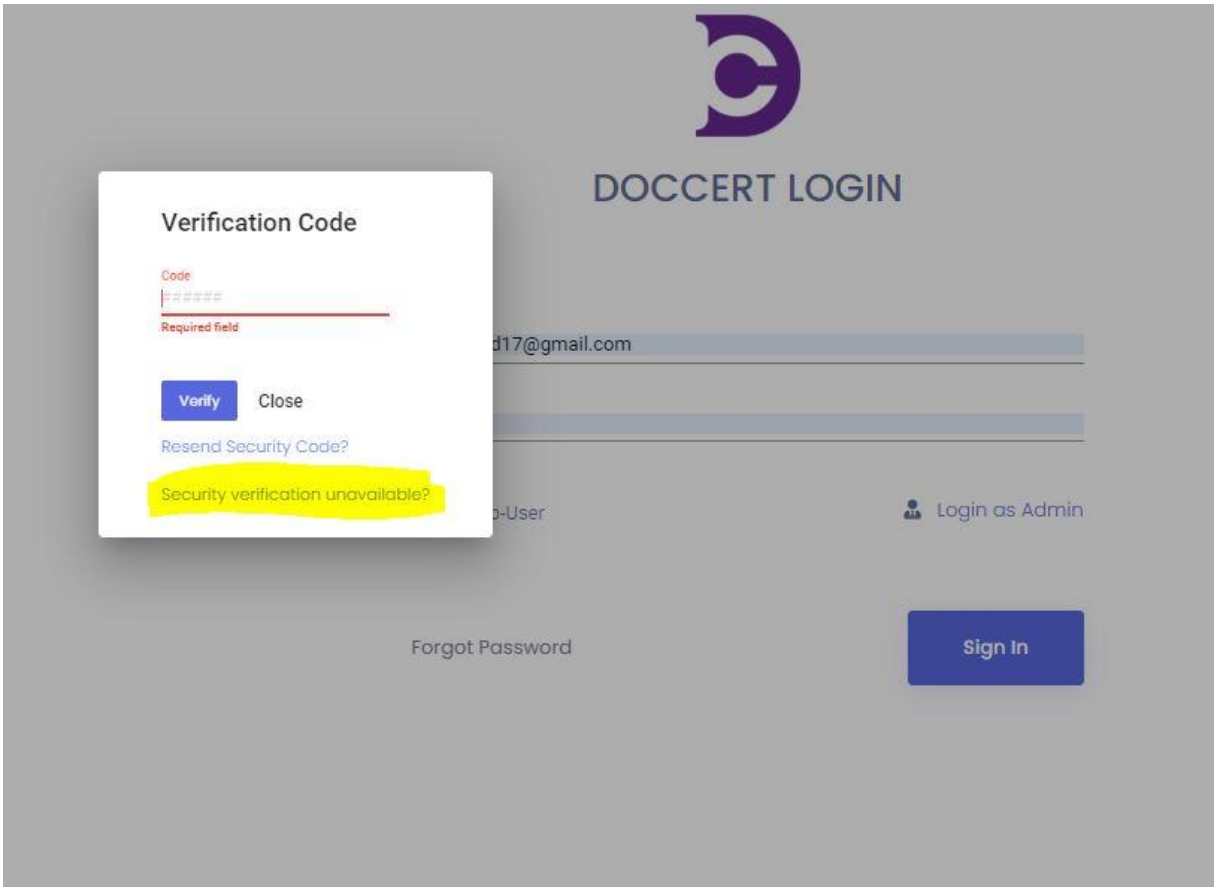


Figure 33:interface authentification échouée

Si l'utilisateur perd son téléphone ou son e-mail, il ne peut pas recevoir le code, il doit donc remplir un formulaire dans lequel il demande de changer son téléphone ou son e-mail et l'envoyer à l'administrateur.



Voilà l'interface de la requête après avoir cliqué sur '' Security verification unvailable ?''

Si l'e-mail ou l'ID utilisateur existe, il peut choisir la méthode en fonction des options qu'il a activées sur son profil.

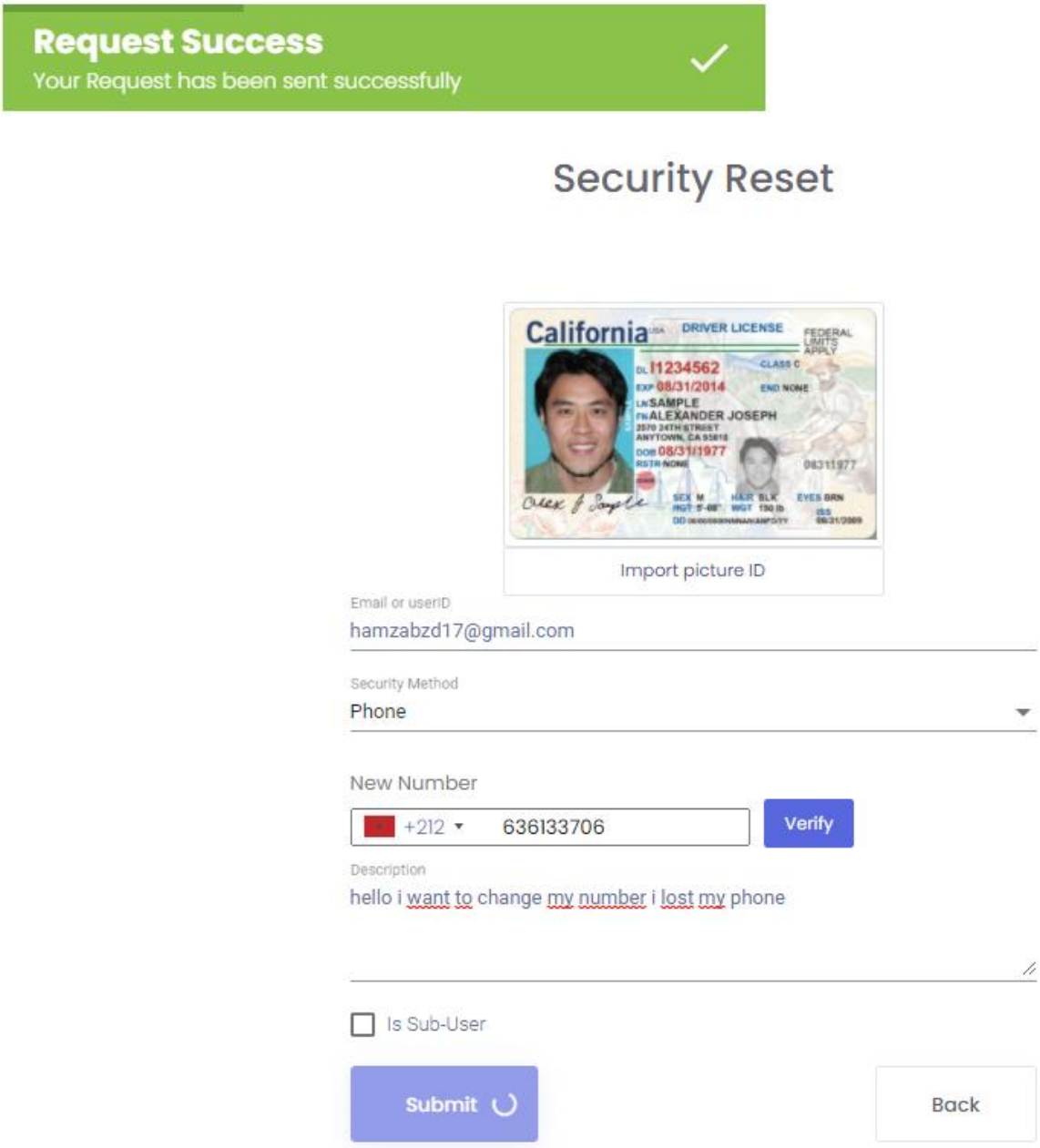


Figure 34:interface de la demande de réinitialisation de la sécurité

Le cas où userID ou l'email n'existe pas.

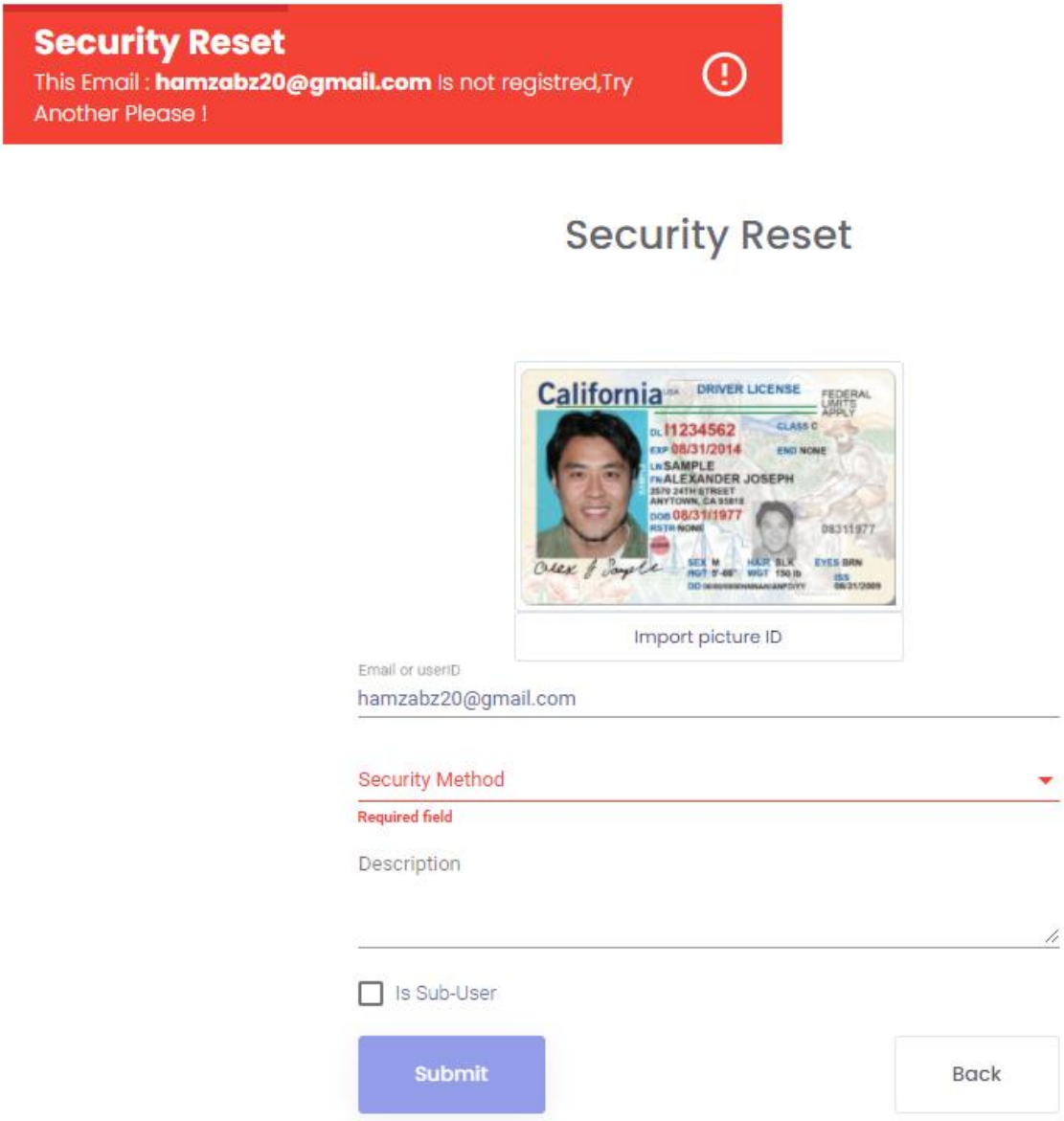


Figure 35 : interface de la demande de réinitialisation de la sécurité au cas d'erreur

L’administrateur liste les demandes, puis il compare la carte d'identité avec les informations de l’utilisateur, si tout est exact il accepte la demande alors le téléphone ou l'email sera mis à jour automatiquement sinon il rejette définitivement la demande.

Ceci est juste une solution temporaire nous utiliserons “seed phrase ” par exemple dans le futur.

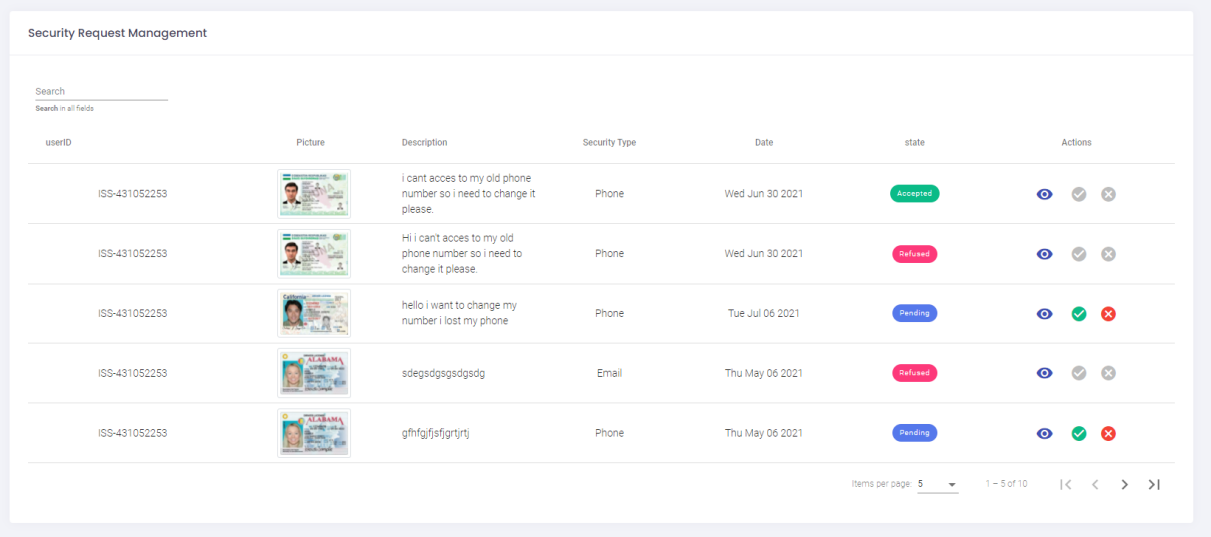


Figure 36: Interface de la liste des demandes de sécurité

L’admin peut Visualiser la demande et faire de la zoom sur la carte d’identité

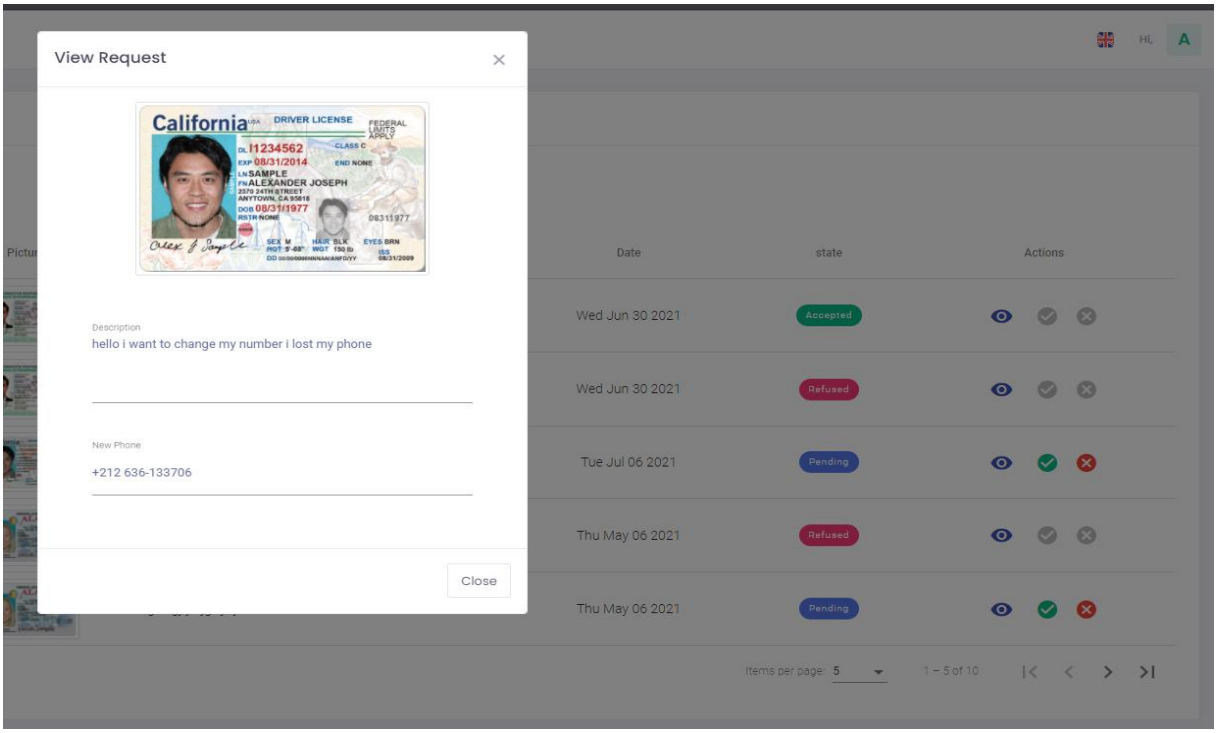


Figure 37: Visualiser la demande de sécurité

3. Cas d’un administrateur d’un organisme (Issuer)

Nous allons traiter les étapes qu’un administrateur d’un organisme doit suivre pour rejoindre un réseau et attribuer des certificats.

Nous avons déjà créé un administrateur de l'organisme qui représente Huwaei dans notre exemple.

Après l’inscription il doit attendre jusqu’à ce que l’administrateur du réseau (Admin) active son compte pour accéder à son tableau de bord.

Voici ci-dessous la liste des demandes d’activation de comptes de plusieurs administrateurs d’organisme.

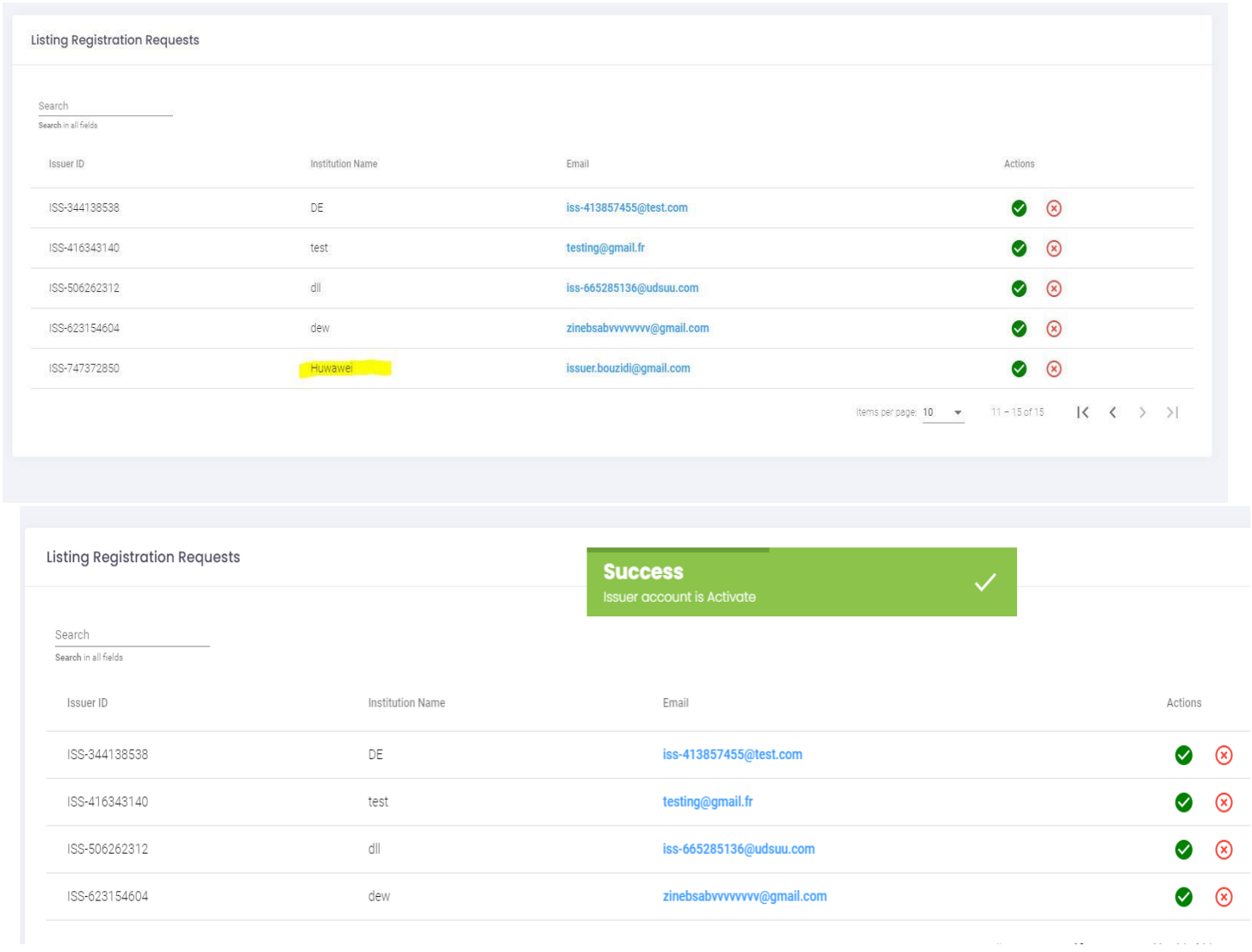


Figure 38:Interface chez l'administrateur du réseau des demandes d'activation de comptes des administrateurs d'organismes.

Après l'activation et l'authentification de l'administrateur de l'organisme(issuer), le système le dirige vers sa page d'accueil qui contient un Dashboard, menu et les activités récentes.

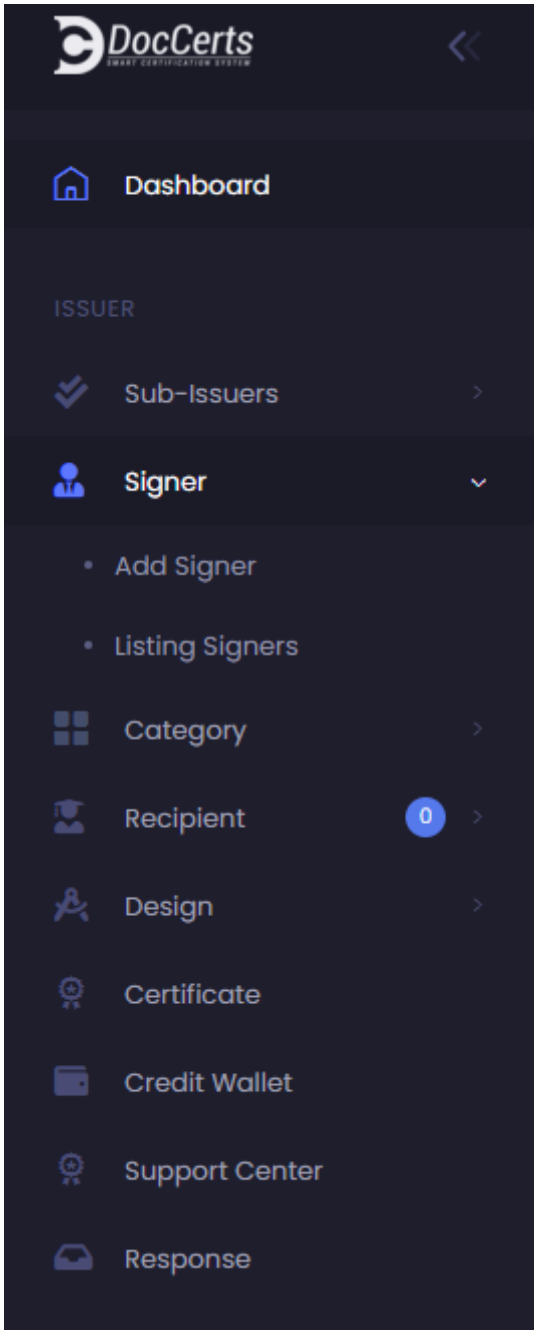


Figure 39:interface du menu de l'administrateur de l'organisme

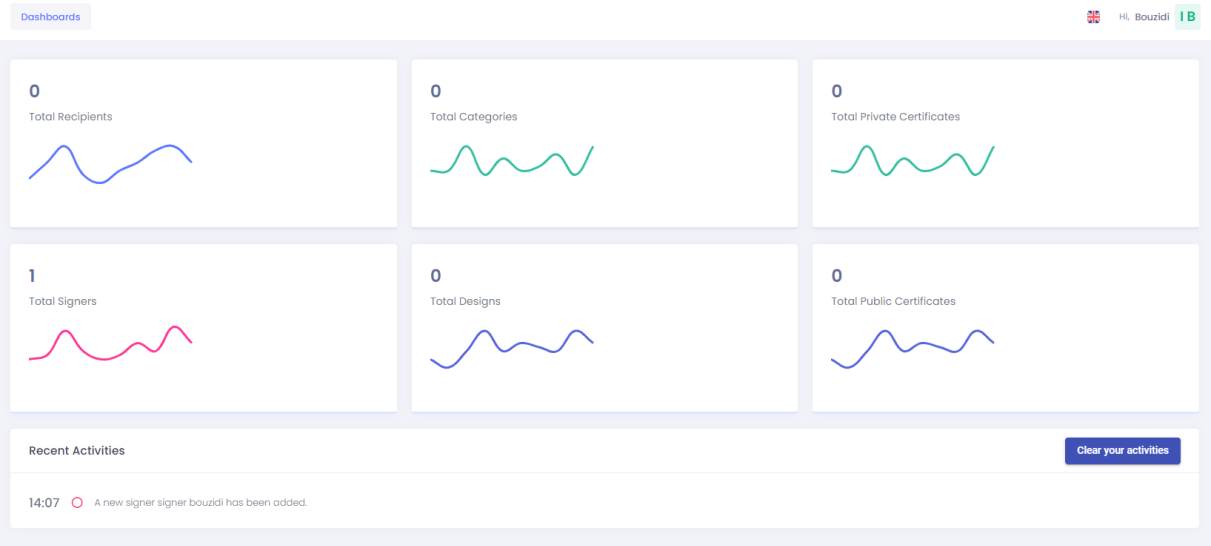


Figure 40 : interface du Dashboard de l'administrateur de l'organisme

tout utilisateur peut suivre ses activités pour voir ce qu'il a fait ce jour-là et peut les effacer à tout moment.

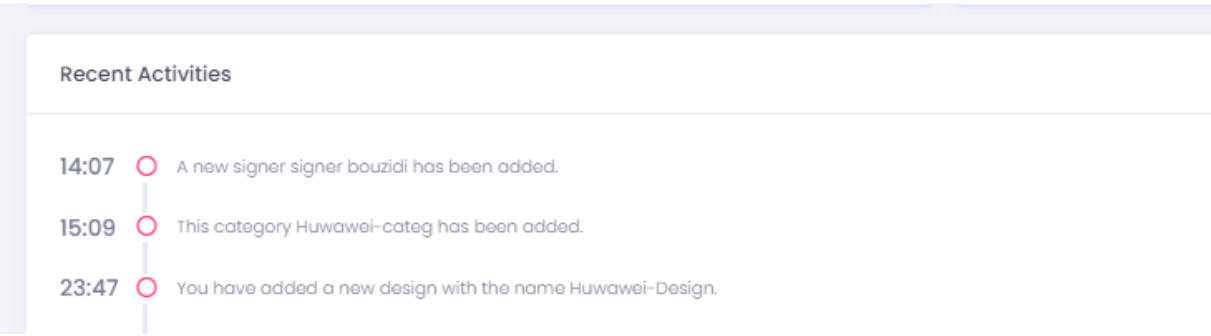


Figure 41: liste des activités récentes

L’administrateur peut ajouter et lister les signataires disponibles.

Ci-dessous est l’interface de l’ajout d’un signataire où l’administrateur de l’organisme doit remplir certains champs pour inviter ce signataire à rejoindre le réseau.

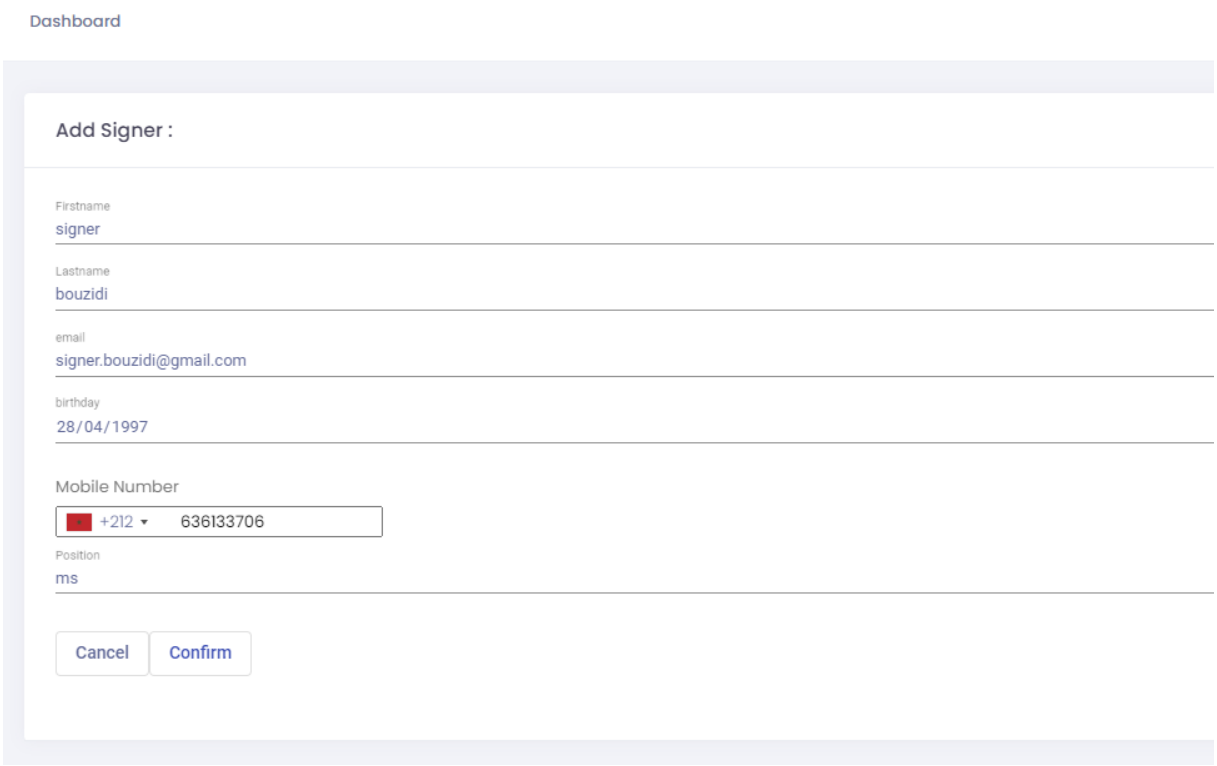


Figure 42: Interface d'ajout d'un signataire

Après l'ajout de ce signataire, une demande d'ajout au réseau a été envoyé par mail et sms au signataire.

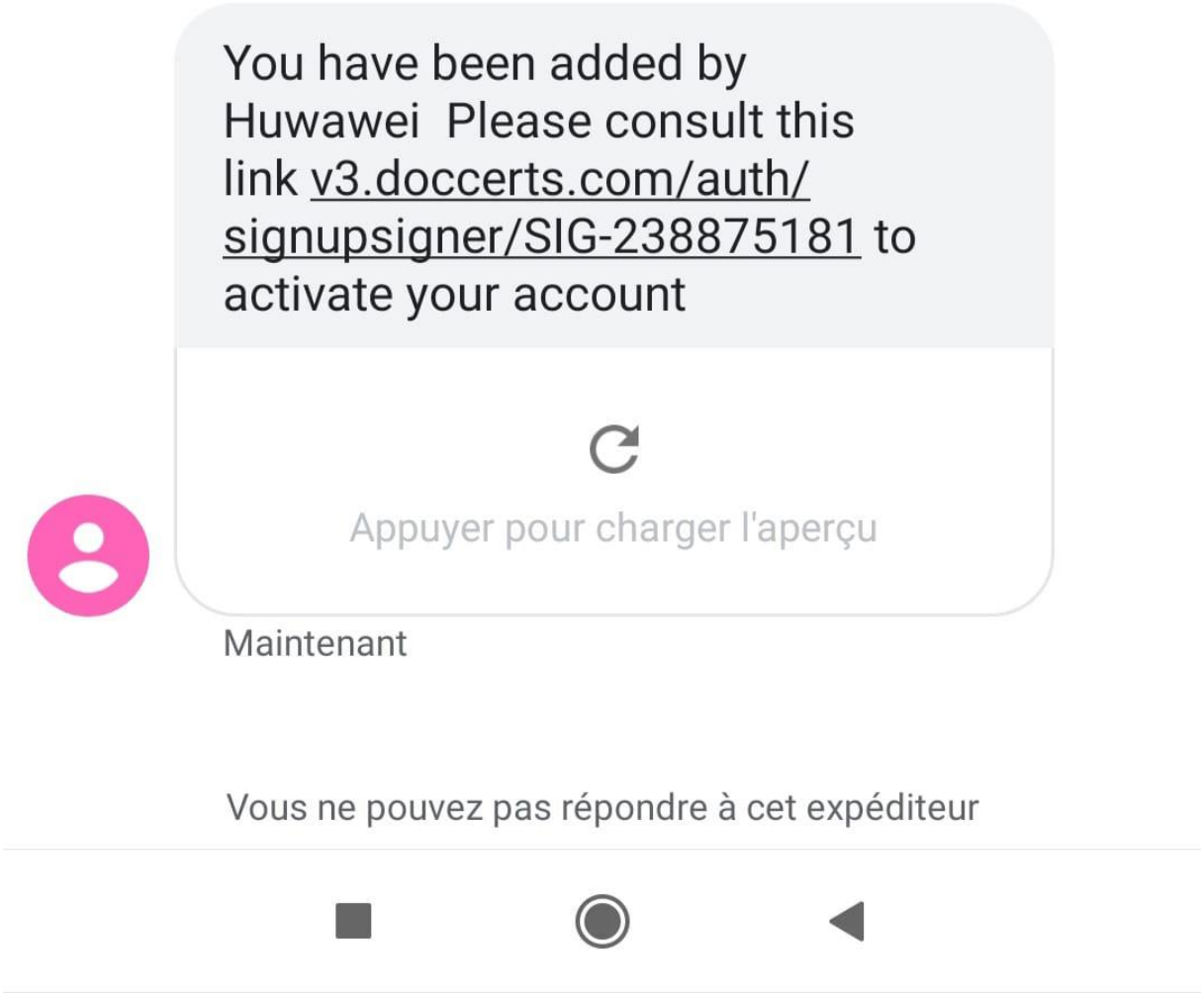


Figure 43: Interface de la demande d'ajout reçu par sms

Ci-dessous la liste des signataires disponible au réseau qui affiche l'état de chaque signataire :

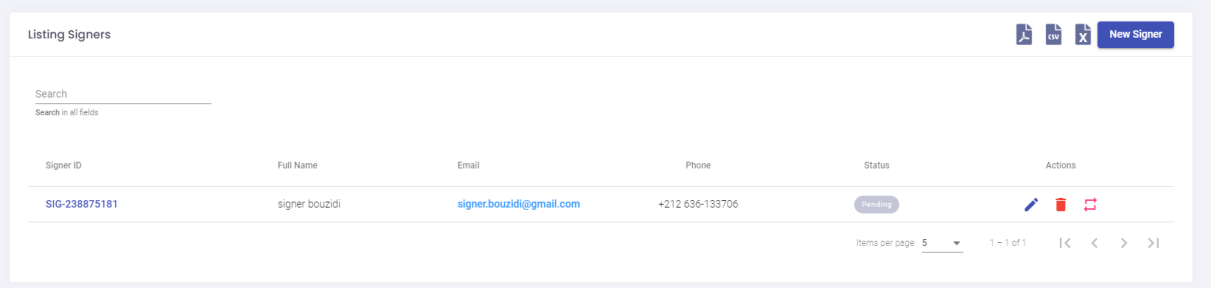


Figure 44:Interface de la liste des signataires (signataire désactivé)

L'administrateur de l'organisme peut mettre à jour les informations du signataire s'il ne s'est pas encore inscrit.

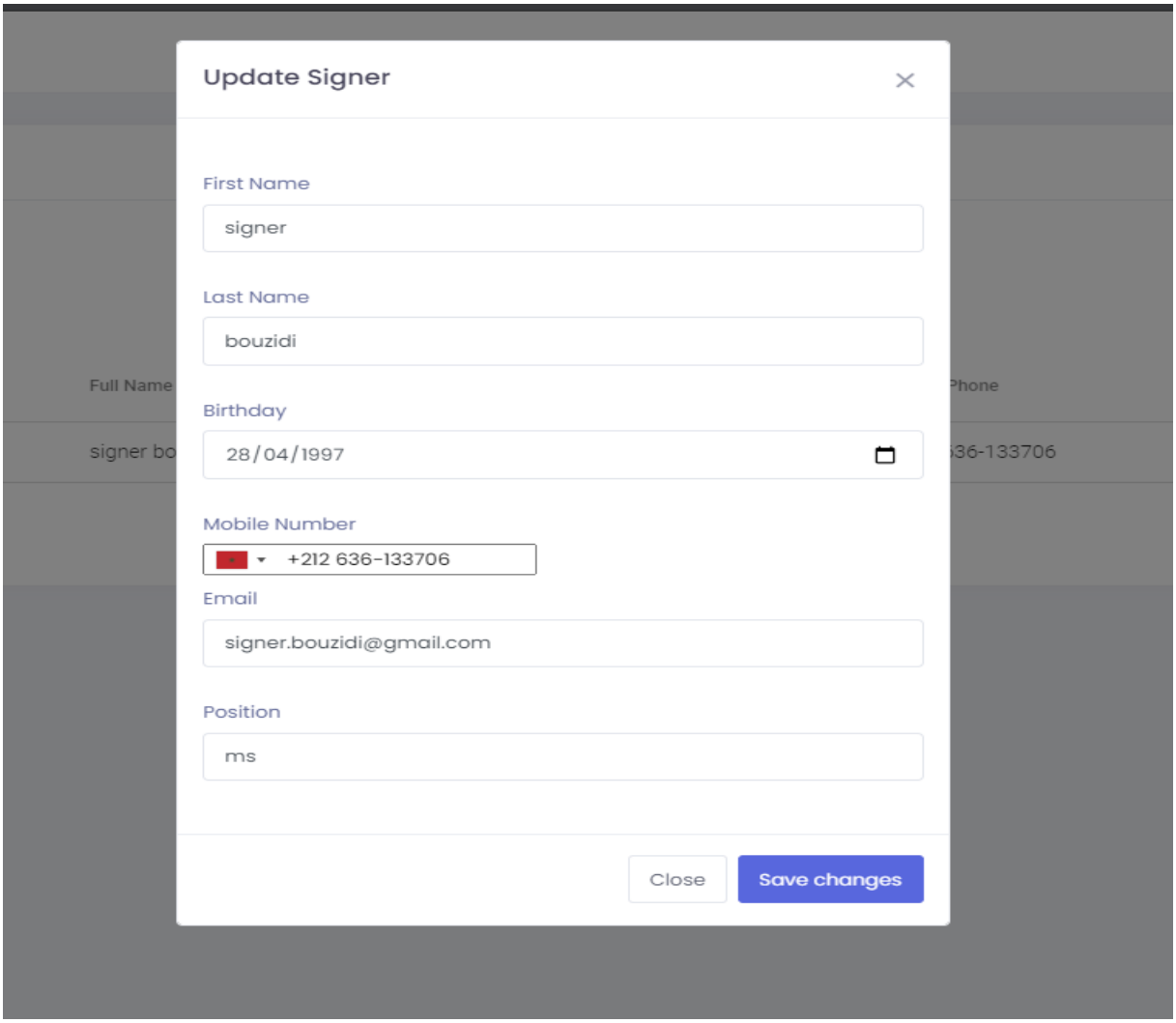


Figure 45:interface de mettre à jour les informations de signataire

Le signataire doit compléter l'inscription via le lien envoyé à son téléphone (figure 51).

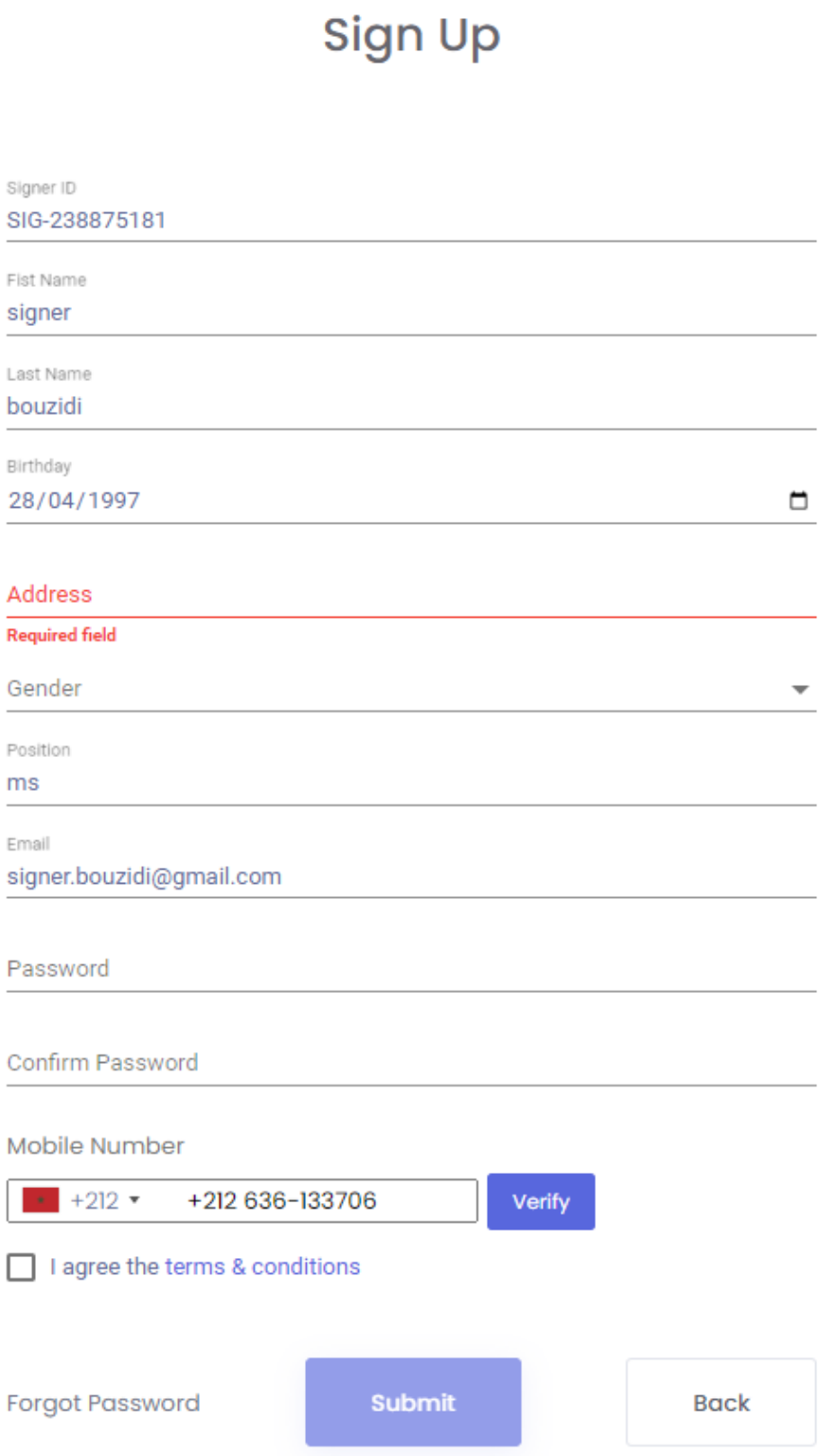


Figure 46: Interface de la complétion de l'inscription du signataire

- **Espace catégorie**

Dans cet espace, l'administrateur peut créer et lister les catégories disponibles.

Dans cet exemple, nous avons ajouté la date d'expiration, la durée et le titre du cours comme champs de certificat et nous avons sélectionné le signataire qui sera le responsable de ce certificat, sans sa signification ce certificat ne peut être vérifié. Nous pouvons aussi sélectionner plus d'un signataire puis nous avons ajouté le nom et prénom du destinataire.

Ci-dessous est l'interface de l'ajout d'une catégorie où l'administrateur de l'organisme doit remplir certains champs.

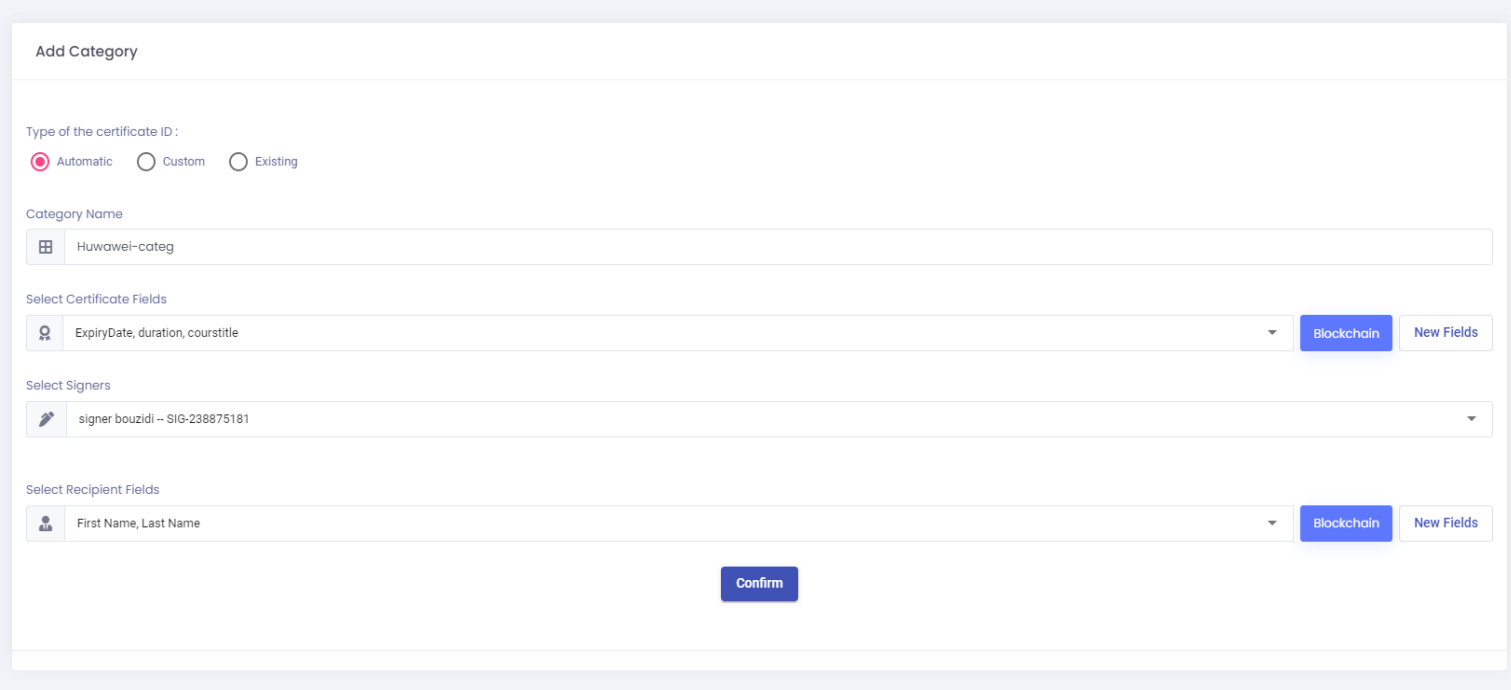


Figure 47: Interface d'ajout d'une catégorie

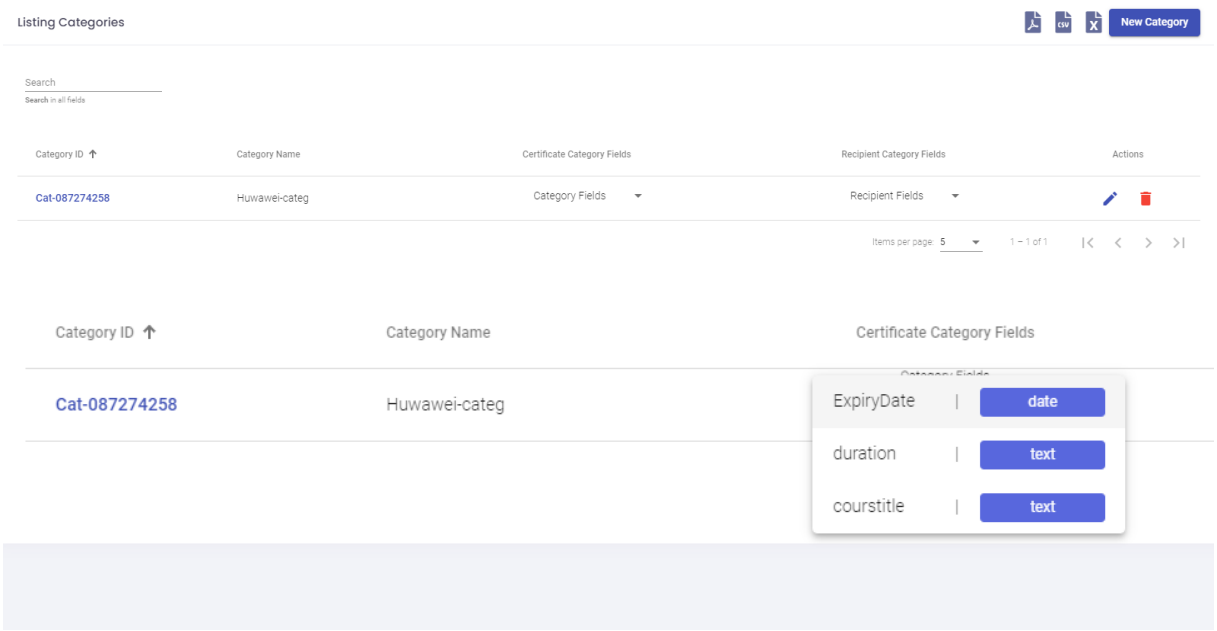
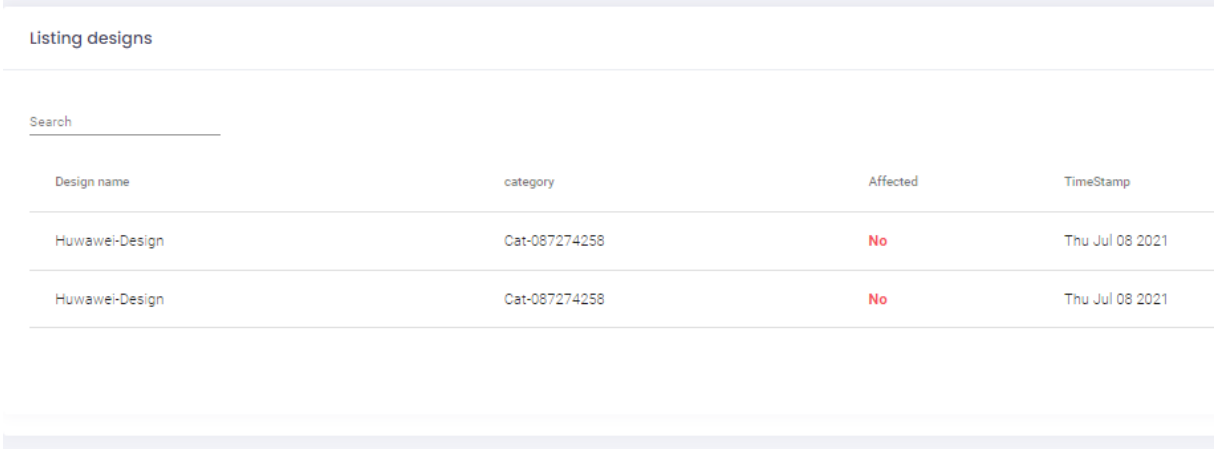


Figure 48:Interface de la liste des catégories

- **Espace Design**

Dans cet espace, l'administrateur peut ajouter et lister les Designs disponibles.

Comme nous pouvons le voir dans la liste de conception, la conception que nous venons de créer n'est pas affectée car nous ne l'avons pas encore utilisée, nous devons encore créer un récepteur et l'affecter à lui



Nous devons d'abord sélectionner une catégorie afin de pouvoir télécharger les champs de l'émetteur, du récepteur et des signataires.

Nous pouvons créer un design simplement en faisant glisser et déposer des champs, des images et des textes par exemple, si nous voulons le prénom et le nom du récepteur sur notre certificat, il nous suffit d'aller dans la section ‘’Recipient Fields ‘’ et de faire glisser les champs dont nous avons besoin.

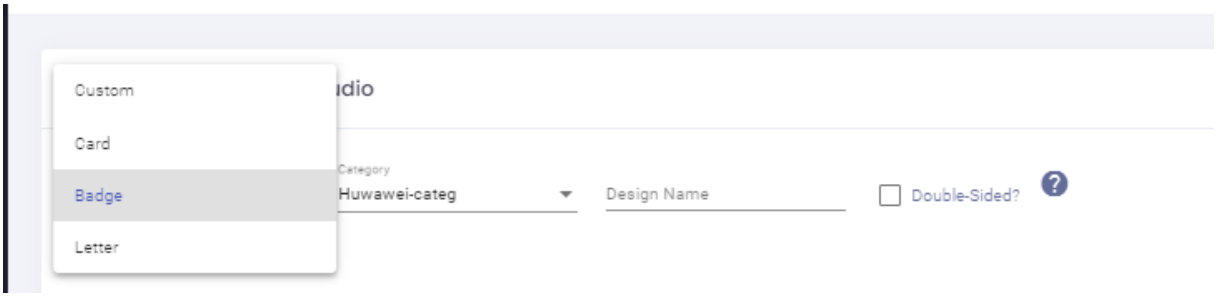


Figure 49: interface de design les types de boîte

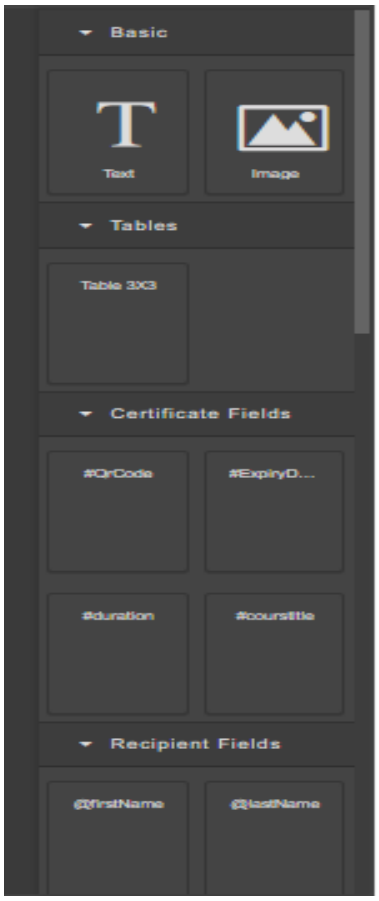


Figure 50 : interface des outils de design

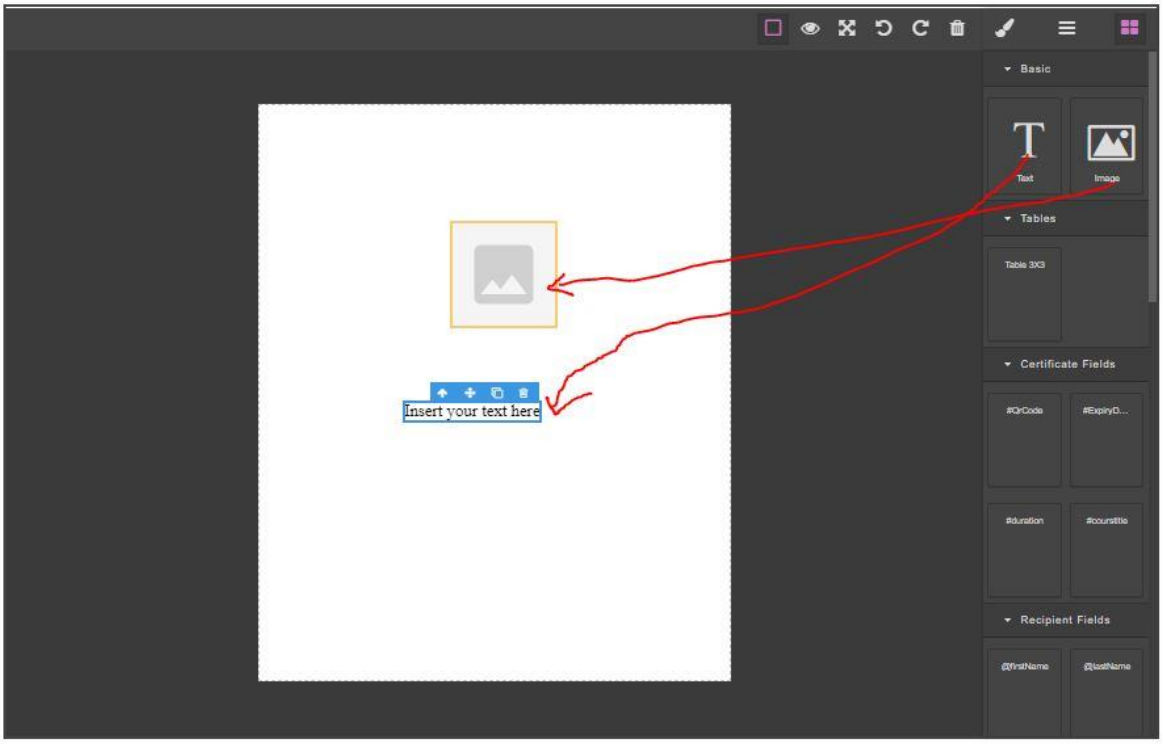


Figure 51: interface du design avec texte et image

L'administrateur de l'organisme peut simplement déposer l'image de son dossier ou passer le lien.

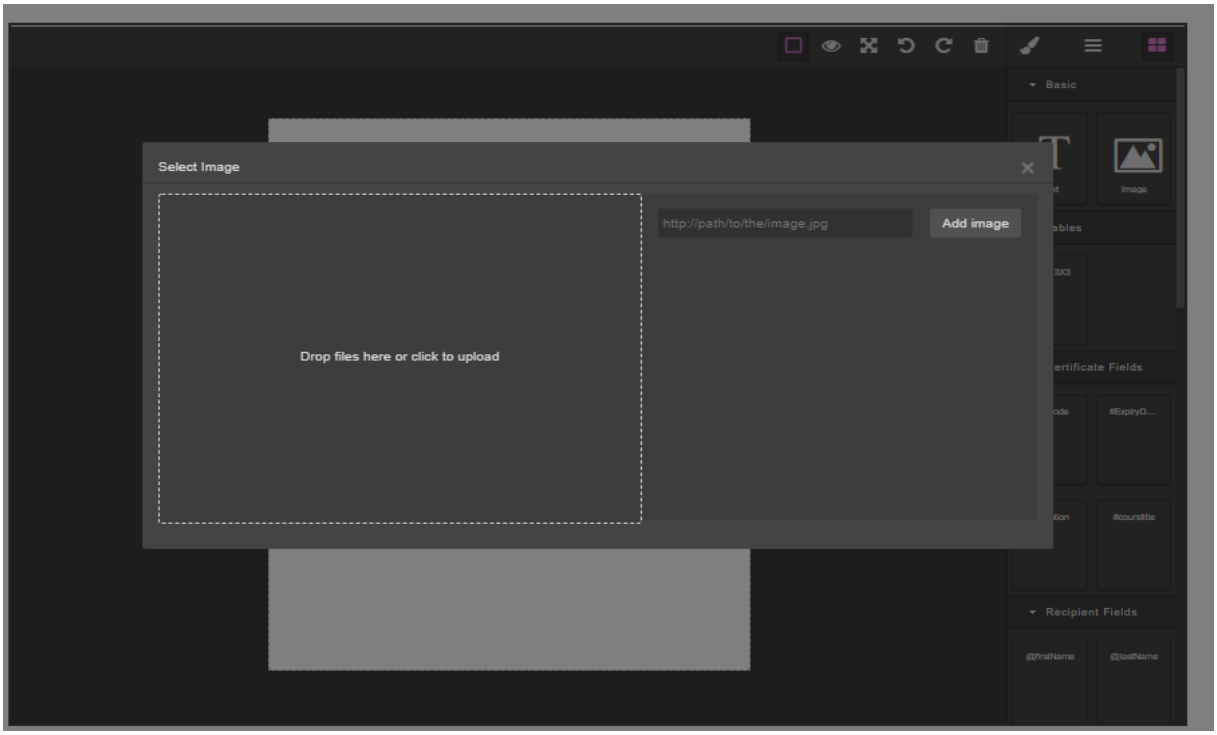


Figure 52 : interface de sélection d'image sur le design

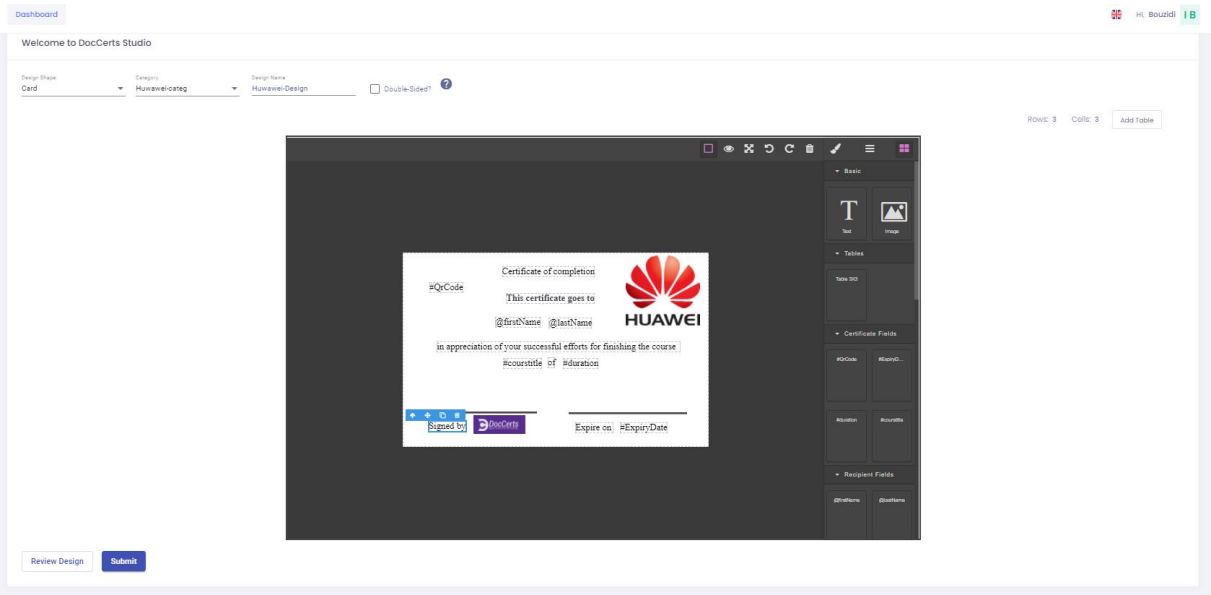
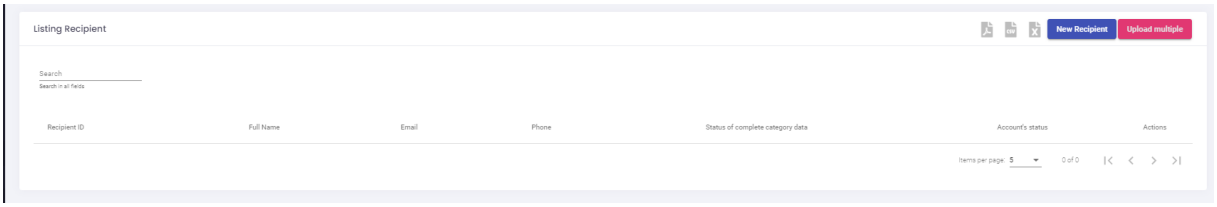


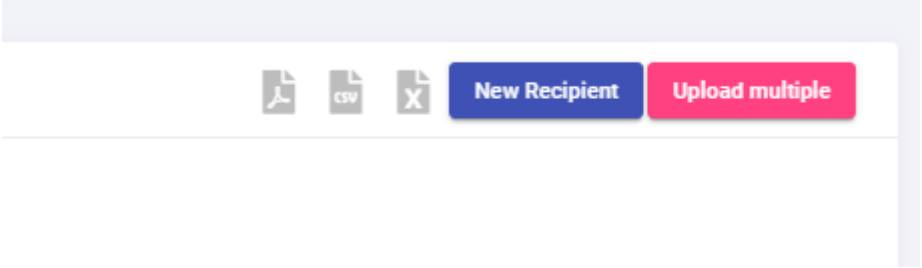
Figure 53:interface de création d'un design de certificat

Figure 54:interface d'un design de certificat

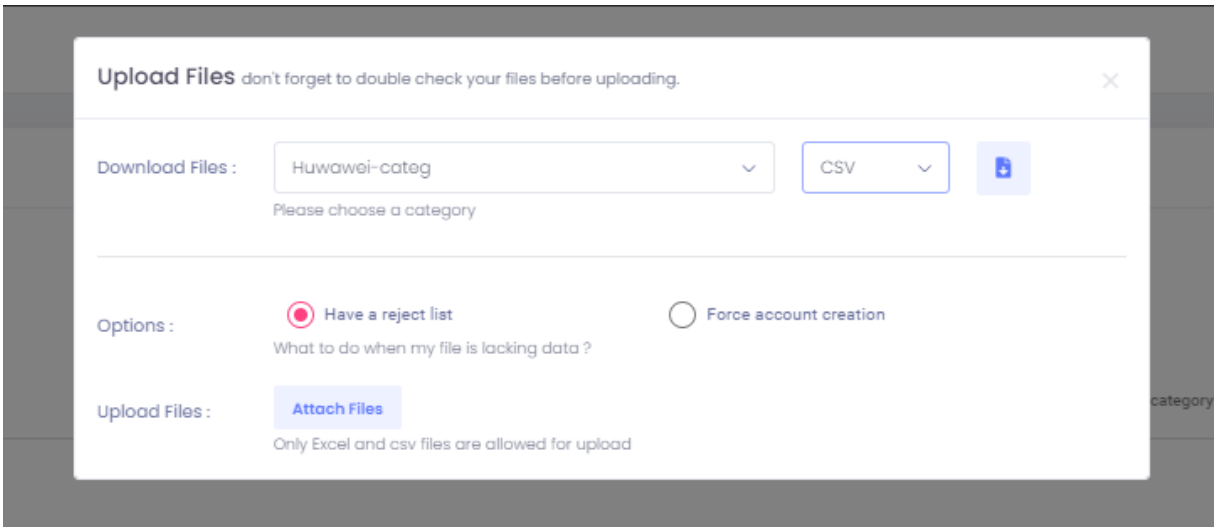
- Espace Récepteur

Dans cet espace, l'administrateur peut inviter et ajouter et lister les récepteurs disponibles.





Nous pouvons créer plusieurs récepteurs à la fois en cliquant sur « upload multiple » où nous devons sélectionner la catégorie et préparer un fichier Excel.



Ci-dessous est l'interface de l'ajout d'un récepteur où l'administrateur de l'organisme doit remplir certains champs.

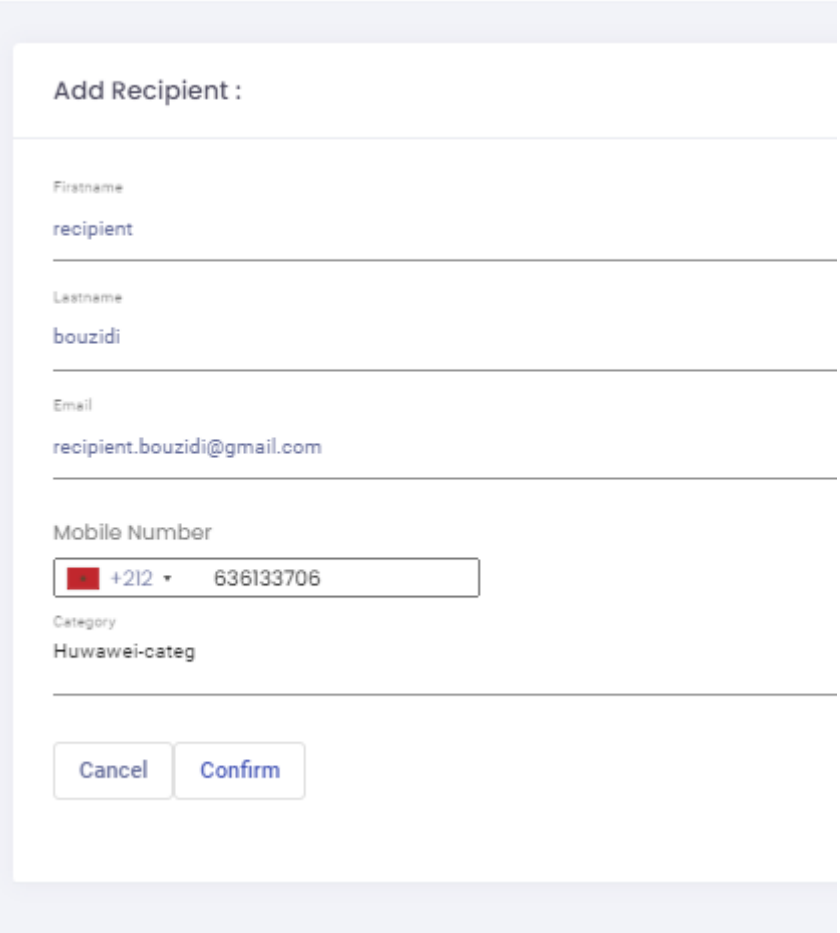


Figure 55: Interface d'ajout d'un récepteur

Après avoir invité le récepteur à rejoindre notre réseau, il recevra un e-mail pour terminer l'inscription où il doit remplir les champs de catégorie que nous lui avons affectés.

Si nous avons ajouté des champs personnalisés comme "Age" pour le récepteur lors de la création de la catégorie, après l'enregistrement il recevra une notification pour entrer les informations d'âge, dans notre exemple nous n'avons pas ajouté de champs personnalisés ,les champs que nous avons ajoutés sont le prénom et le nom ils sont requis par défaut comme nous le voyons sur la figure 60.

Figure 56:Interface de la notification du remplissage des données chez le récepteur

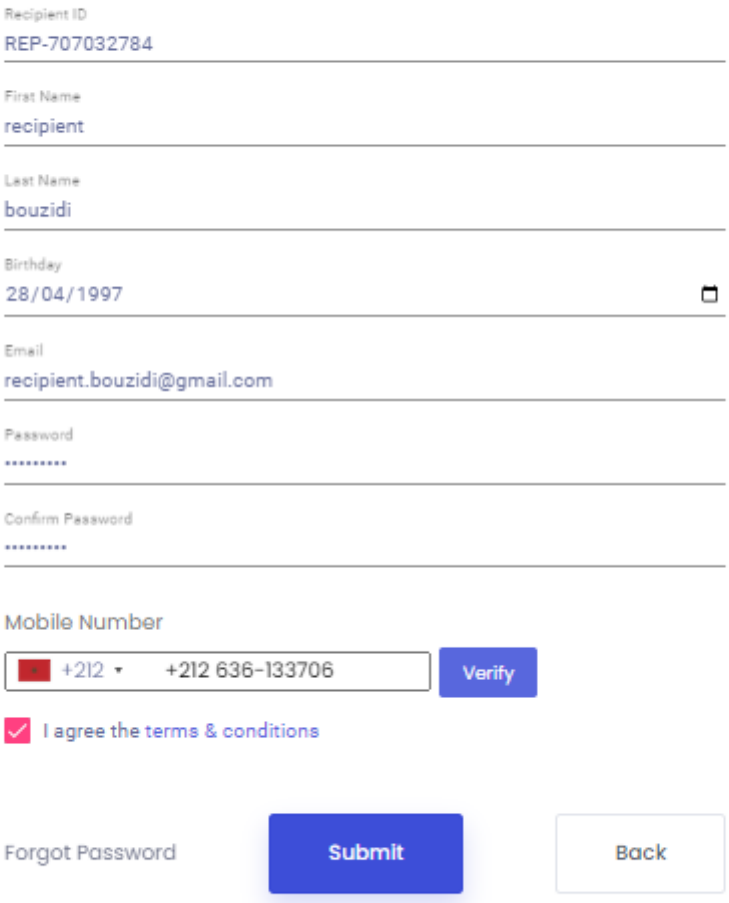


Figure 57:interface d'inscription d'un récepteur

Le récepteur peut lister ses catégories, dans cet exemple nous voyons que le statut est actif car le destinataire a rempli les champs de catégorie requis.

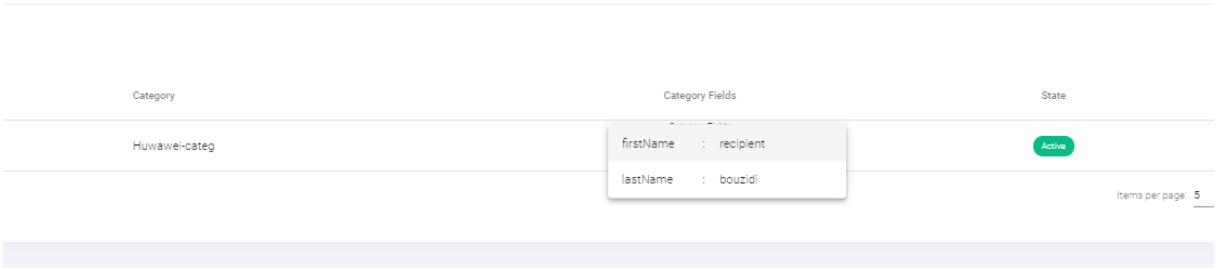
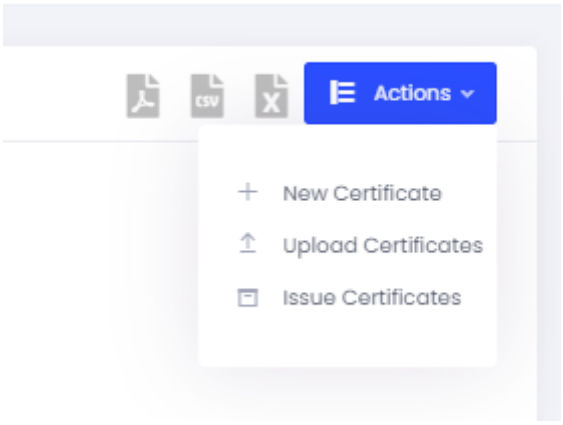
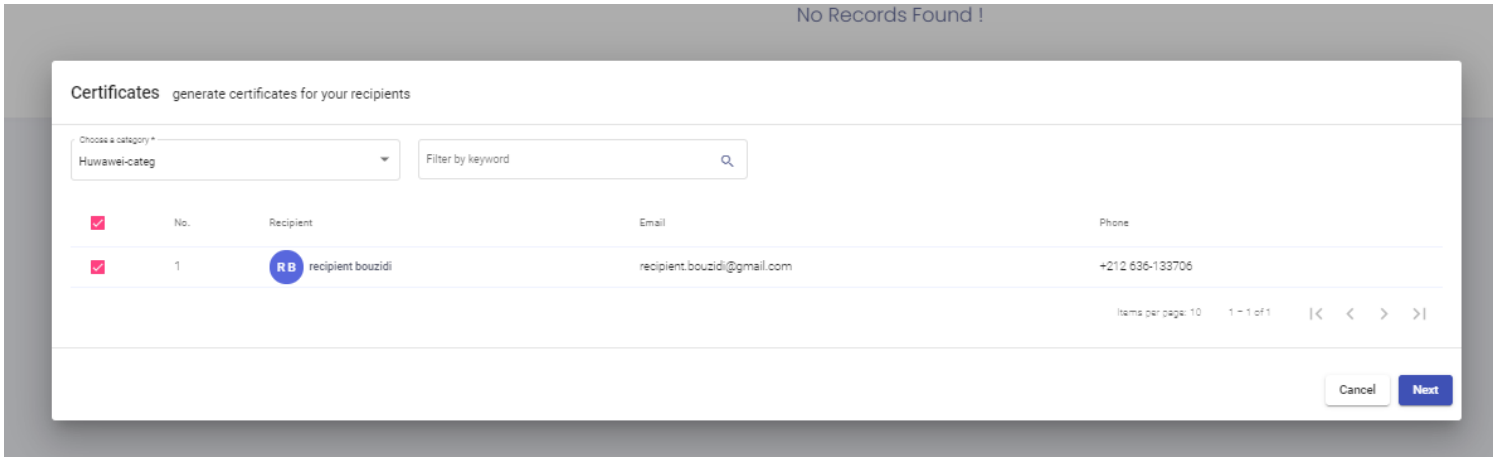


Figure 58:interface de la liste des catégories chez le récepteur

L'administrateur de l'organisme doit générer des certificats pour ses récepteurs



Pour créer le certificat, l'administrateur de l'organisme doit d'abord choisir le récepteur.



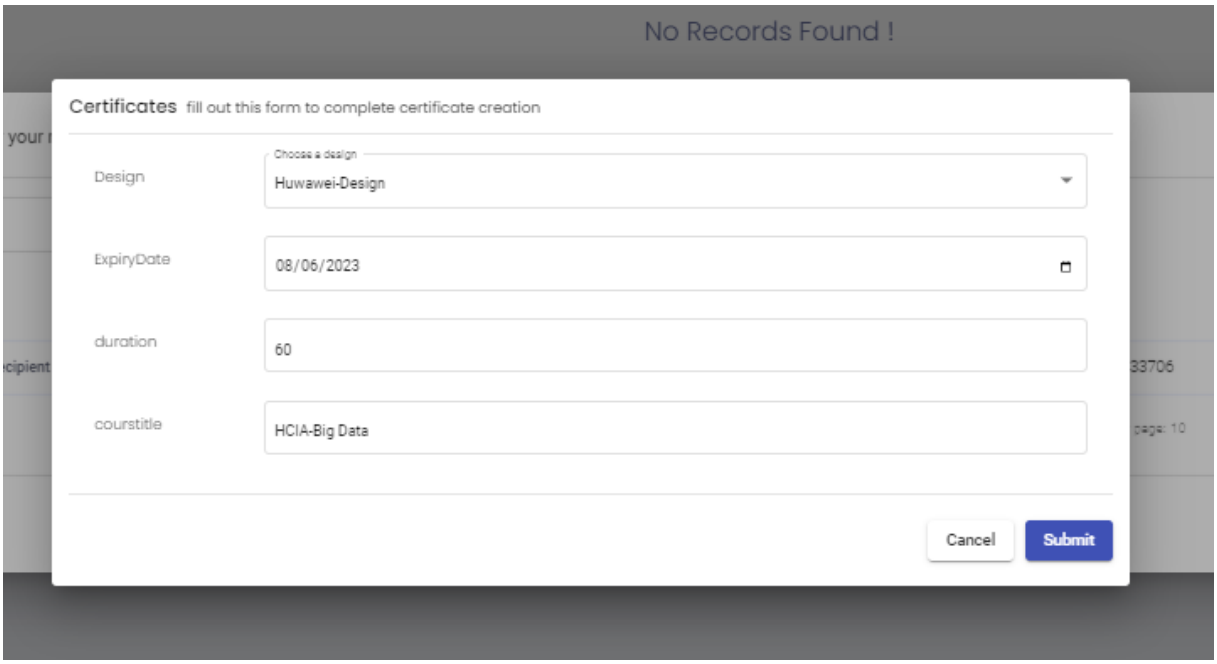


Figure 59:interface de création du certificat

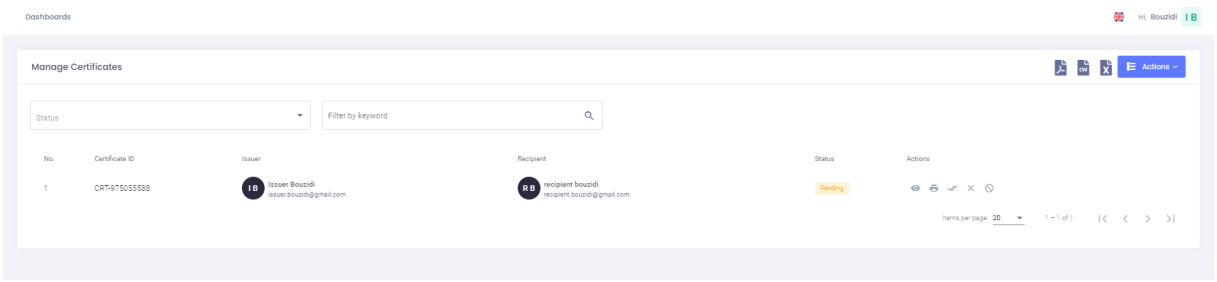


Figure 60:interface de la liste des certificats chez l'administrateur de l'organisme

Avant d'émettre le certificat, le signataire doit d'abord signer le.

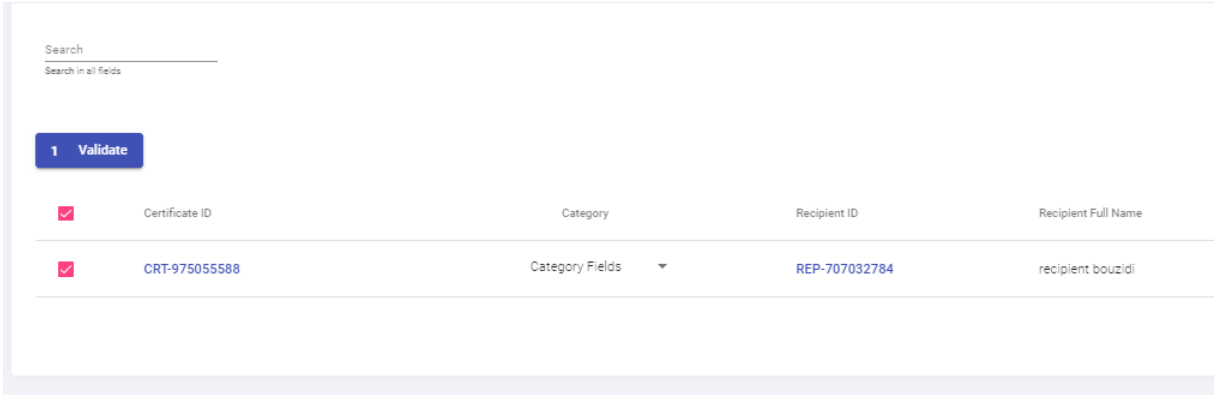


Figure 61:interface de la validation du certificat par le signataire

L’administrateur de l'organisme doit choisir où émettre le certificat, en réseau privé ou en réseau public.

Pour le réseau privé, uniquement les membres du réseau d’organisme qui pourra voir la transaction.

Pour le réseau public tout le monde peut voir la transaction.

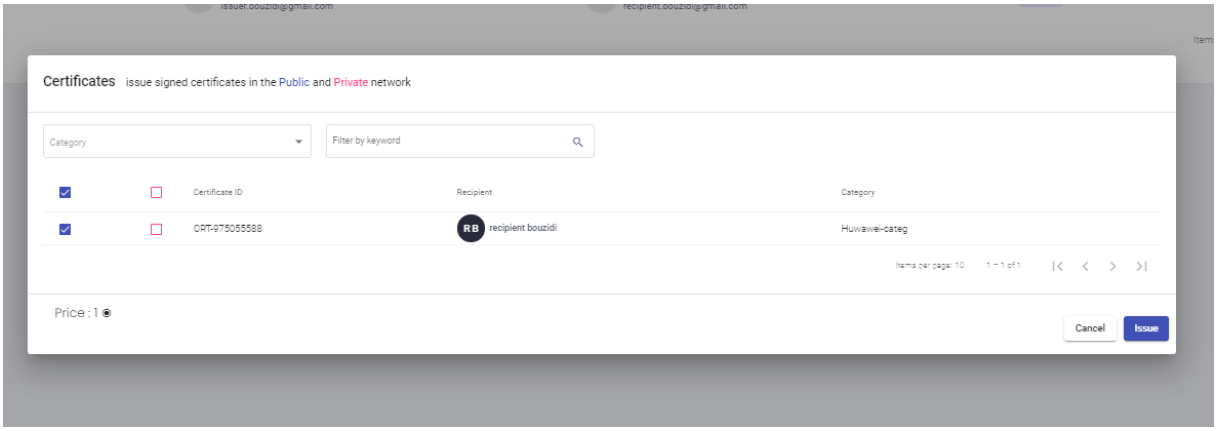


Figure 62:interface d'émettre le certificat vers le réseau prive

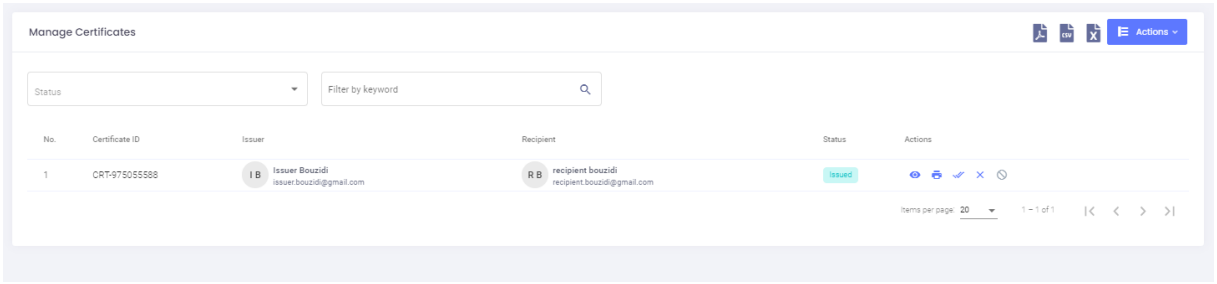


Figure 63: interface de la liste des certificats issued

Ci-dessous est l'interface où nous pouvons voir et vérifier le certificat.

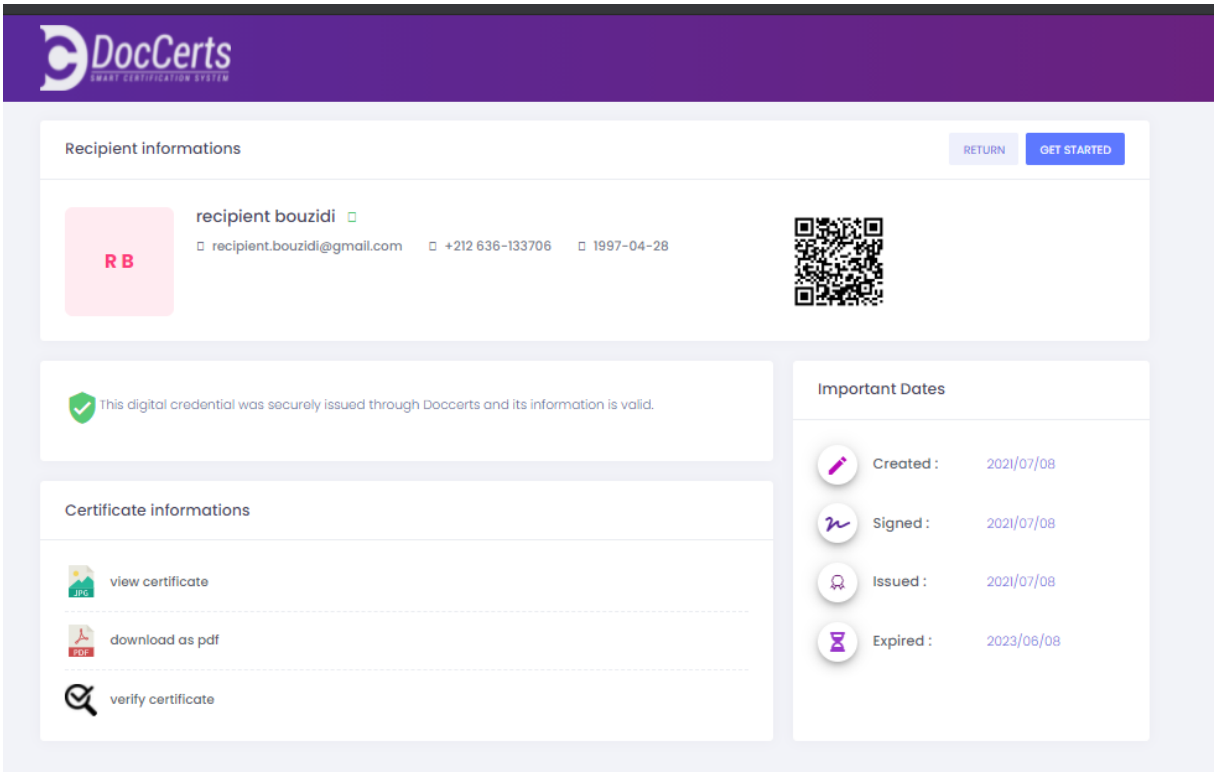


Figure 64: interface pour vérifier le certificat

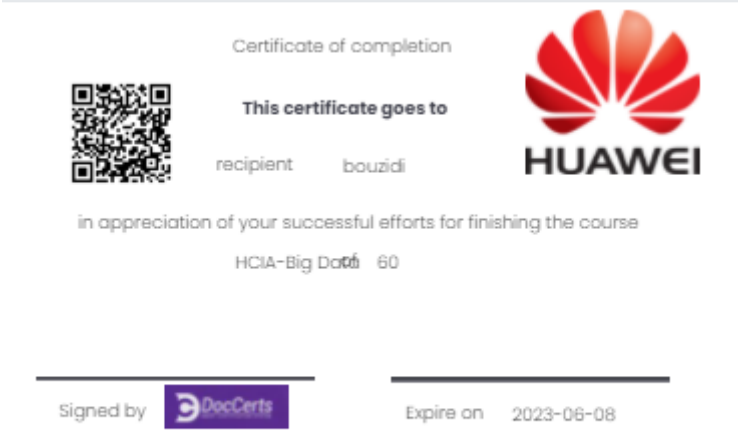


Figure 65 : Interface du certificat du récepteur

La vérification passe par 4 étapes :

1- Vérifier si le certificat n'a pas été falsifié.

2- Vérifier si le certificat n'a pas expiré.

3- Vérifier si le certificat non révoqué par l'émetteur.

4- Vérification de l'authenticité.

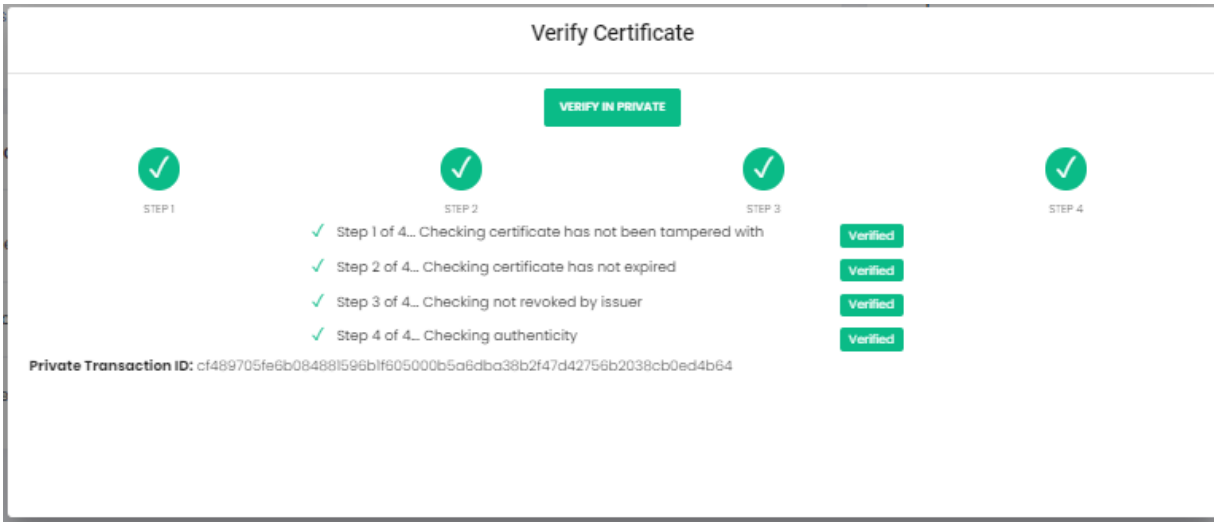


Figure 66:interface de vérification du certificat

Nous pouvons vérifier le certificat en scannant le code QR par téléphone.

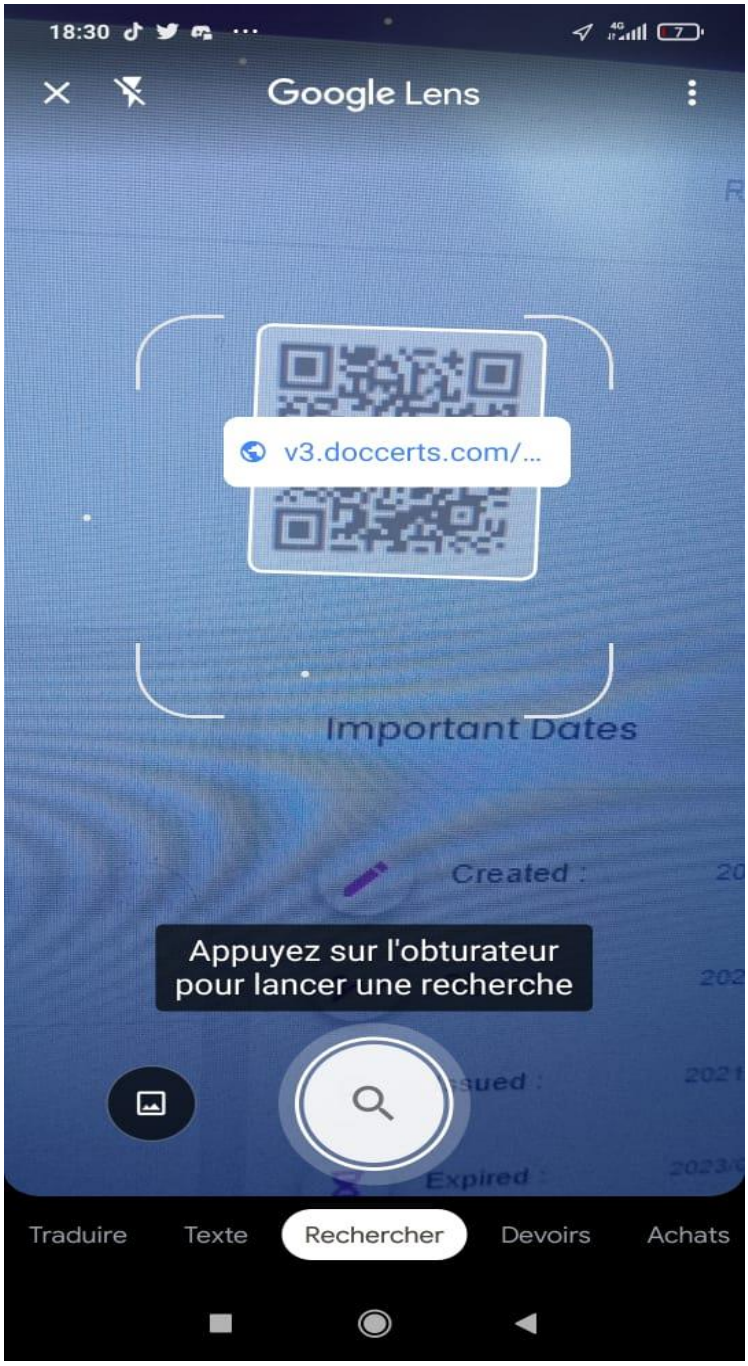


Figure 67:capture d'écran du téléphone scanne QR code du certificat

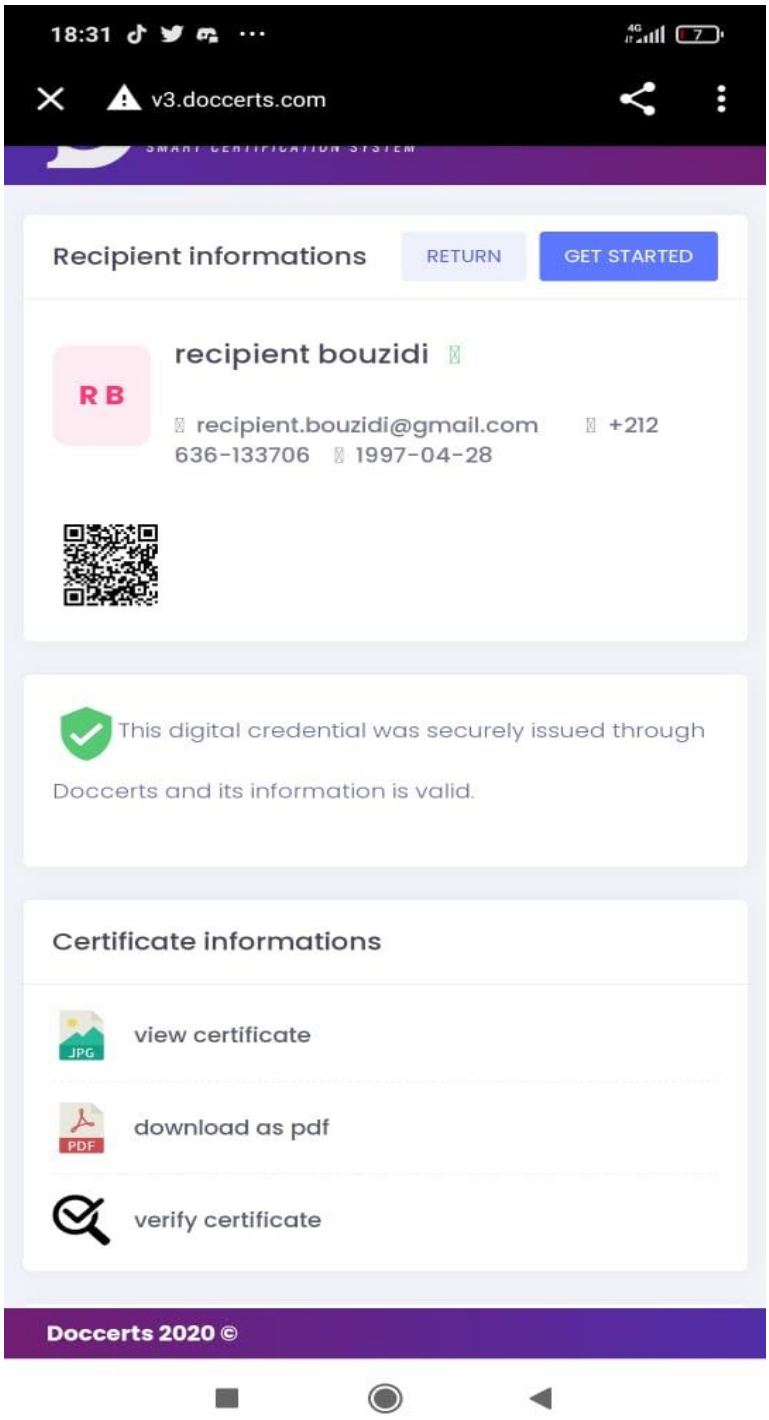


Figure 68 : interface pour vérifier le certificat sur téléphone

3.1. Quelques interfaces de la nouvelle version

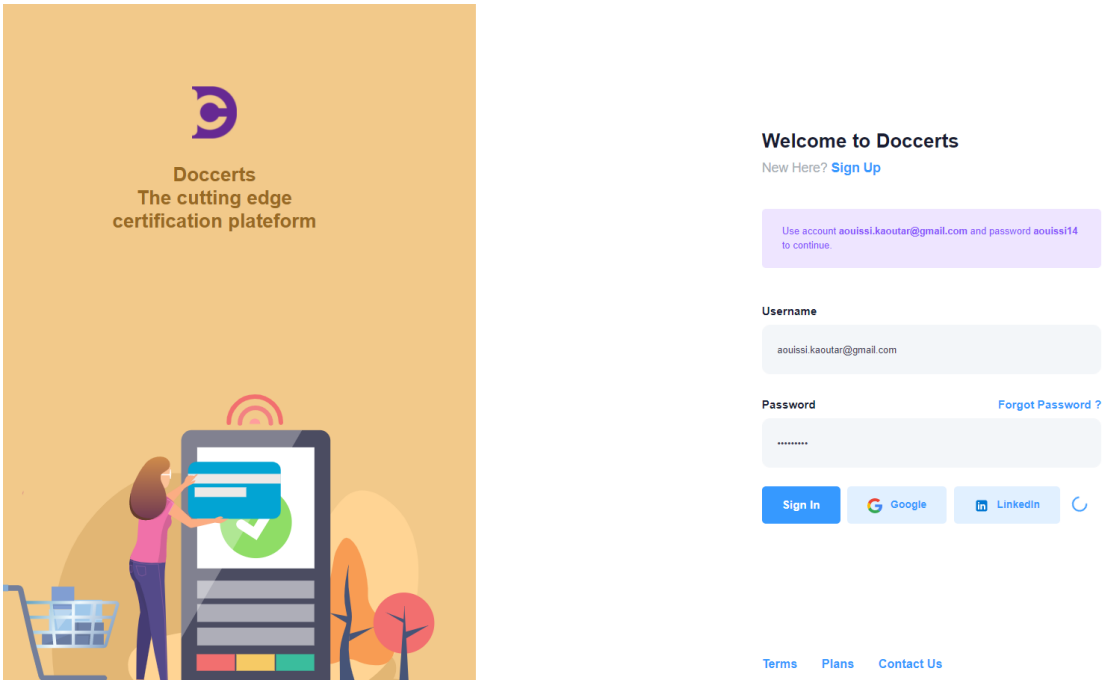


Figure 69:interface d'authentification de la nouvelle version

- Espace d'administrateur de l'organisme

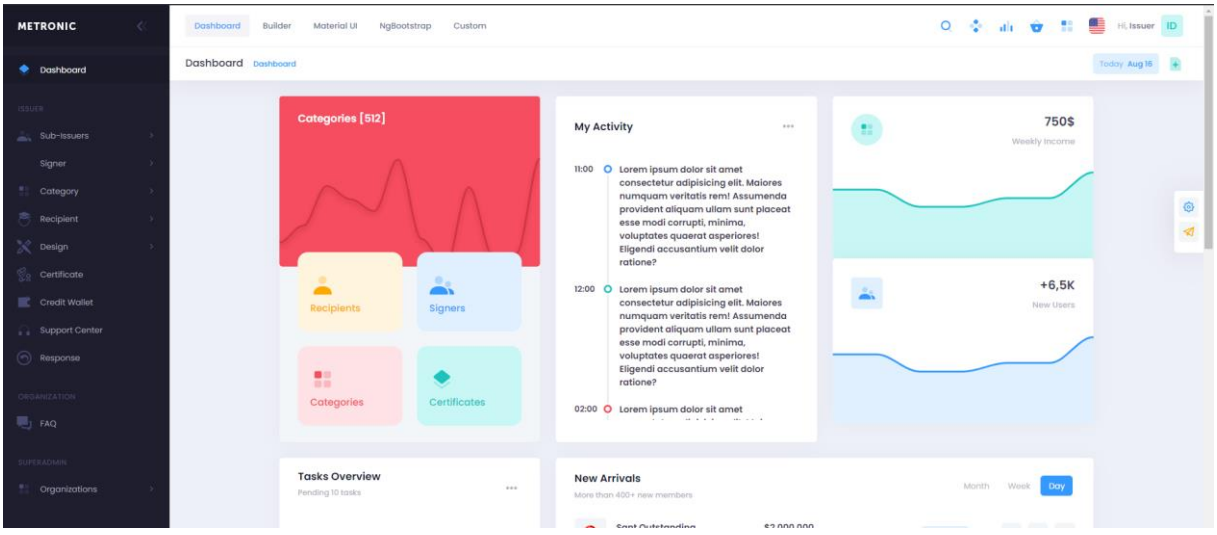


Figure 70 : interface de Dashboard chez issuer

La plupart de ces composants (table, dialogue, formulaires) sont réutilisables, par exemple si l'un des développeurs a besoin de construire une table pour lister les certificats, il peut appeler la table par sa balise html et spécifier les noms des colonnes.

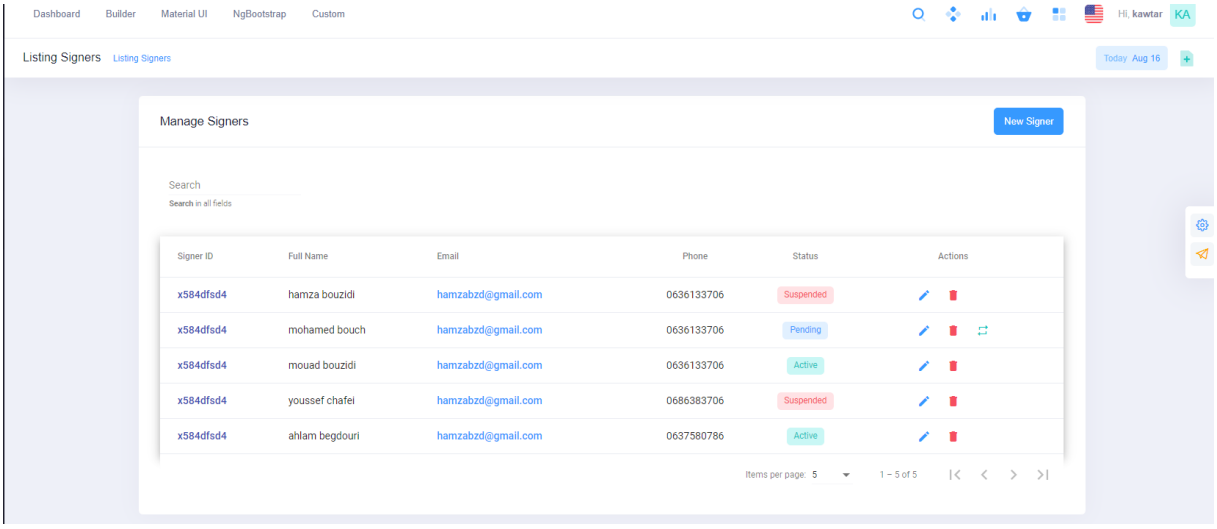


Figure 71: interface de la liste des signataires

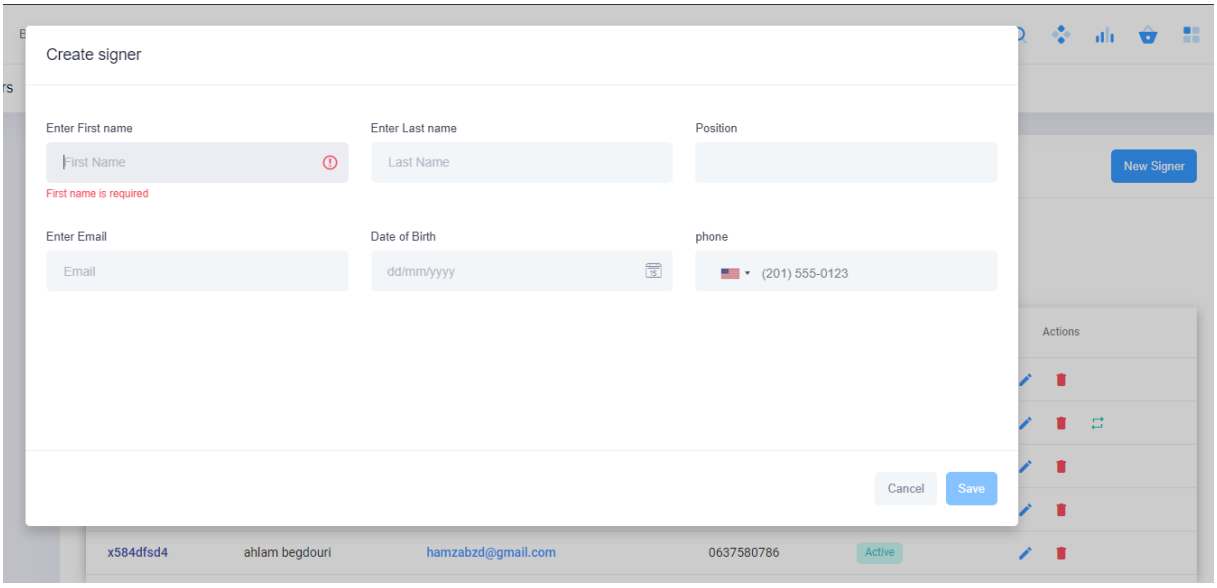


Figure 72 : interface de création d'un signataire

Conclusion

Nous avons effectué notre stage de fin d'études à la société Smart Transformation, dans ce stage nous avons eu l'occasion de travailler avec des technologies modernes sur une application qui permet de signer et vérifier des documents officiels.

L'application contient plusieurs outils qui visent à traiter les documents officiels, de la création jusqu'à la vérification, et cela a pour but d'aider les utilisateurs à recevoir des documents personnalisés selon l'organisme, et d'avoir ces documents signés et stockés dans la Blockchain pour qu'ils soient plus être sécurisés et facile à les vérifier.

Nous avons pu utiliser et améliorer nos compétences sur des nouvelles langages de programmation où nous avons appris à développer un frontend avec angulaire pour bien optimiser les pages Web (''single page application ''), Nous avons aussi appris comment gérer une base de données en temps réel avec firebase. Nous avons également eu l'occasion de travailler sur la nouvelle version de l'application où nous avons appris à créer des composants réutilisables avec angulaire, comment bien organiser le code, nous avons également programmé avec Spring Boot comme backend où nous avons appris à gérer les exceptions et communiquer les micro-services entre eux, aussi à gérer Les requête no SQL avec mongodb repositories.

En outre, ce stage était, pour nous, une occasion de mettre en pratique nos connaissances acquises et notre savoir-faire, de se rapprocher des difficultés du marché de travail, et vivre une expérience professionnelle valorisante et encourageante pour nous dans l'avenir.

Webographie

[1] https://www.researchgate.net/publication/335174-Blockchain 2019/04/05

[2] https://www.trufflesuite.com/docs/truffle 2020/07/23

[3] https://www.blockchainhub.net 2020/04/18

[4] https://www.euderka.co/blockchain 2020/08/24

[5] https://www.trufflesuite.com/guides/ethereum-overview 2021/01/15

[6] https://www.trufflesuite.com/guides/ethereum-guide 2021/01/15

[7] https://www.researchgate.net/publication/335174-Blockchain 2019/04/05

[8] Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives.

[9] https://angular.io/guide/what-is-angular 2020/08/15

[10]https://www.tutorialspoint.com/spring_boot/spring_boot_introduction.htm 2020/04/13

[11]https://www.edureka.co/blog/hyperledger-vs-ethereum/#whatethereum2021/02/10

[12] https://aws.amazon.com/fr/what-is-aws/ 2019/03/18

[13] https://www.twilio.com/the-current/what-is-twilio-how-does-it-work 2020/04/14

[14] https://keenthemes.com/metronic-theme/ 2021/03/15

[15] https://grapesjs.com/ 2019/07/12

[16] https://www.trufflesuite.com/docs 2021/05/17

[17] https://www.hyperledger.org/learn/research 2018/07/15

Application décentralisée basée sur la blockchain pour la signature et la vérification des Documents(front-end)

Résumé

La validation des documents constitue un obstacle majeur à l'échelle internationale, tenant compte des délais et procédures complexes qu'ils doivent endurer.

En outre, la fraude des diplômes et des certificats (tout autre type de document), constitue un risque majeur et n'a pas un impact seulement sur la crédibilité du système d'éducation mais aussi pour le simple citoyen.

L'objectif de ce travail est la signature et la vérification automatique des documents en maximisant la sécurité afin d'éviter toute difficulté rencontrée lors de la réutilisation de ces documents et aussi éliminer le risque de fraude.

Mots clés : Blockchain, diplôme, étudiant, signature, vérification, université, recruteur.

Decentralized application based on the blockchain for the signature and verification of documents (front-end)

Abstract

The validation of documents is a major obstacle at the international level, taking into account the delays and complex procedures they have to endure.

In addition, the fraud of diplomas and certificates (or any other type of document) constitutes a major risk and has an impact not only on the credibility of the education system but also for the ordinary citizen.

The objective of this work is the automatic signature and verification of documents by maximizing the security in order to avoid any difficulty encountered during the reuse of these documents and also eliminate the risk of fraud.

Keywords: Blockchain, diploma, student, signature, verification, university, recruiter.

Master Systèmes Intelligents & Réseaux

Département d'Informatique

Faculté des Sciences et Techniques de Fès

A.U. 2020 - 2021