Chapitre 1

Analyse et Spécification des Besoins

Introduction

Dans la genèse d'un projet, la phase de spécification et d'analyse des besoins représente une étape fondamentale. Elle permet de définir avec précision les attentes des utilisateurs et les exigences que le système doit satisfaire. Pour initier cette phase, nous menons une étude approfondie des applications existantes en matière de gestion d'identité numérique et de lutte contre la fraude. Cette analyse minutieuse nous aide à identifier les éléments clés et les lacunes à combler avec notre solution. Au cours de cette démarche, nous formulons les exigences fonctionnelles et non fonctionnelles du projet, posant ainsi les bases solides pour le développement d'Identity Secure. Nous introduisons également les premières contraintes de conception, illustrées par le diagramme de cas d'utilisation. Enfin, nous présentons la méthodologie qui guidera l'ensemble du processus de développement.

1. Contexte & problématique

Dans cette section, nous offrons une vue d'ensemble détaillée de notre projet de fin d'études. Nous expliquons le contexte dans lequel il s'inscrit, les motivations qui ont conduit à son élaboration, ainsi que la problématique centrale que nous cherchons à résoudre.

1. Contexte

Le projet, intitulé "Identity Secure : une plateforme innovante pour la gestion d'identité numérique et la lutte contre la fraude", s'inscrit dans le cadre de notre mémoire de fin d'études pour l'obtention du diplôme de Licence Nationale en sciences de l'Informatique (LNI) délivré par l'Institut Supérieur d'Informatique de Mahdia (ISIMa). Ce projet professionnel est réalisé sur une période de quatre mois, du 1er février 2024 au 31 mai 2024, au sein de l'entreprise Twyn-T4ISB :

https://www.t4isb.com

Figure 1 : Logo de l'entreprise d'accueil

2. Problématique

Dans un contexte où la gestion des identifiants fiscaux, tels que le CPF (Cadastro de Pessoas Físicas), est essentielle pour prévenir les fraudes et garantir l'intégrité des systèmes financiers et sociaux, les organisations sont confrontées à des défis majeurs. Les fraudes massives impliquant des CPF multiples ou usurpés pour bénéficier illégalement d'aides sociales ou effectuer des transactions frauduleuses sont devenues un problème récurrent, notamment au Brésil.

Les processus traditionnels de gestion des identités numériques présentent souvent des lacunes significatives, telles que des inefficacités opérationnelles, des erreurs humaines et des difficultés à garantir la conformité aux normes et réglementations en constante évolution. Une des principales difficultés réside dans la complexité croissante des systèmes d'information, accentuée par l'évolution des technologies et la numérisation des processus commerciaux. Cette complexité compromet la qualité globale de la gestion des identités et la réactivité des organisations face aux problèmes identifiés.

Face à ces défis, il est impératif pour les organisations de repenser leurs approches en matière de gestion d'identité numérique et d'explorer des solutions innovantes pour simplifier et optimiser ces processus. L'automatisation des tâches répétitives, l'utilisation de technologies émergentes telles que la reconnaissance biométrique, et le renforcement des mesures de sécurité et de confidentialité des données sont des pistes à explorer pour relever les défis actuels de la fraude et assurer la pérennité des systèmes d'identité dans un environnement économique en perpétuelle évolution.

2. Etude de l'existant

L'étude de l'existant permet de déterminer les points faibles et les points forts d'un produit actuel pour déterminer les besoins du client, en vue d'en prendre en considération lors de la conception et la réalisation de notre plateforme.

2.1 Revue des solutions existantes

Suite à une étude approfondie du marché, plusieurs solutions existantes en matière de gestion d'identité numérique et de lutte contre la fraude ont été identifiées. Ces solutions offrent généralement des fonctionnalités telles que la vérification biométrique, la gestion des identifiants uniques et la détection des fraudes. Cependant, elles présentent souvent des limites en termes de convivialité, d'automatisation et d'intégration avec les systèmes existants. Voici une analyse des produits les plus populaires dans ce secteur : **e-Estonia, IDEMIA, Onfido** et **Serpro.**

2.1.1 e-Estonia (Estonie)

e-Estonia est une plateforme numérique utilisée en Estonie pour la gestion des identités numériques des citoyens. Lancée en 2002, elle permet aux utilisateurs d'accéder à des services gouvernementaux en ligne de manière sécurisée grâce à une carte d'identité numérique et une signature électronique.

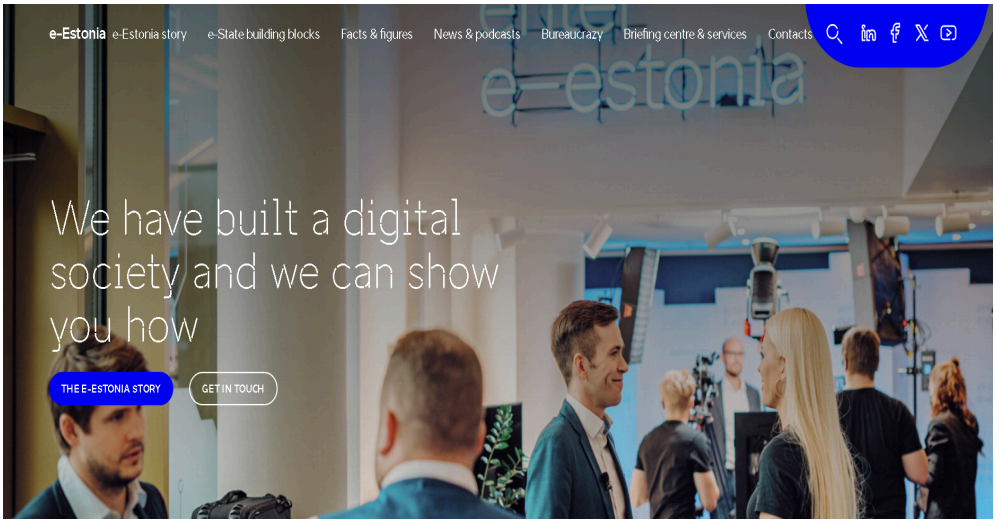

Figure 2 : Page d'accueil de « e-Estonia »

Processus d'utilisation :

- Les citoyens estoniens obtiennent une carte d'identité numérique, qui sert de clé d'accès aux services en ligne.
- La plateforme permet de signer des documents électroniquement, de voter en ligne,et d'accéder à des services de santé et d'éducation.
- Les données sont stockées de manière décentralisée, ce qui renforce la sécurité et la confidentialité.

Acteurs :

- Gouvernement estonien : Responsable de la gestion et de la maintenance de la plateforme.
- Citoyens : Les utilisateurs finaux qui utilisent leur carte d'identité numérique pour accéder aux services.
- Entreprises et institutions : Les entités qui intègrent e-Estonia pour offrir des services en ligne.

Points forts :

- Décentralisation des données, ce qui améliore la sécurité.
- Large éventail de services accessibles en ligne.

Points faibles :

- Forte dépendance à l'égard de l'infrastructure gouvernementale.
- Difficulté à adapter le système à d'autres pays en raison de sa spécificité.

2.1.2 IDEMIA (Solution Globale)

IDEMIA est une entreprise spécialisée dans les technologies d'identification biométrique. Elle propose des solutions pour la gestion des identités numériques, notamment dans les secteurs bancaires et gouvernementaux. Fondée en 2017, IDEMIA est présente dans plus de 180 pays et offre des solutions basées sur la reconnaissance faciale, les empreintes digitales, et l'iris.

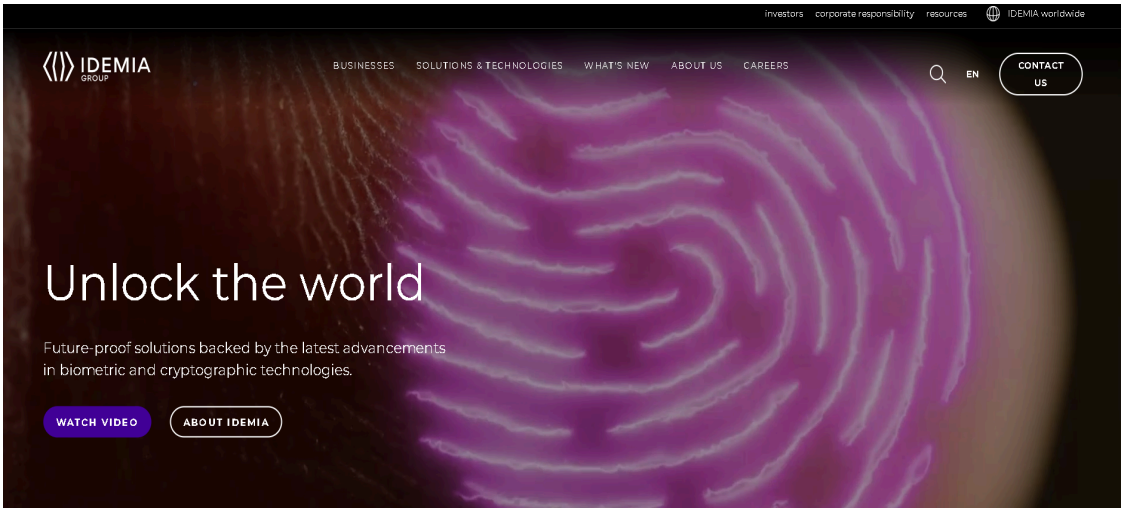

Figure 1.4 : Page d'accueil de « IDEMIA »

• Processus d'utilisation :

- Les utilisateurs s'enregistrent auprès des institutions partenaires (banques, gouvernements) en fournissant leurs données biométriques.
- Les données sont stockées dans une base de données sécurisée et utilisées pour vérifier l'identité des utilisateurs lors des transactions.
- Les institutions peuvent intégrer les solutions d'IDEMIA via des API pour automatiser les processus de vérification.

• Acteurs :

- IDEMIA : L'entreprise qui développe et maintient les solutions biométriques.
- Institutions partenaires : Les banques, gouvernements et entreprises qui utilisent les solutions d'IDEMIA.
- Utilisateurs finaux : Les citoyens ou clients qui utilisent les services basés sur l'identification biométrique.

• Points forts :

- Technologies biométriques avancées.
- Large portée internationale.

• Points faibles :

- Complexité d'intégration avec les systèmes existants.
- Coût élevé de mise en œuvre.

2.1.3 Onfido (Royaume-Uni)

Onfido est une plateforme de vérification d'identité basée sur l'intelligence artificielle. Elle utilise la reconnaissance faciale et la vérification de documents pour authentifier les utilisateurs. Fondée en 2012, Onfido est principalement utilisée par les entreprises privées pour vérifier l'identité de leurs clients.

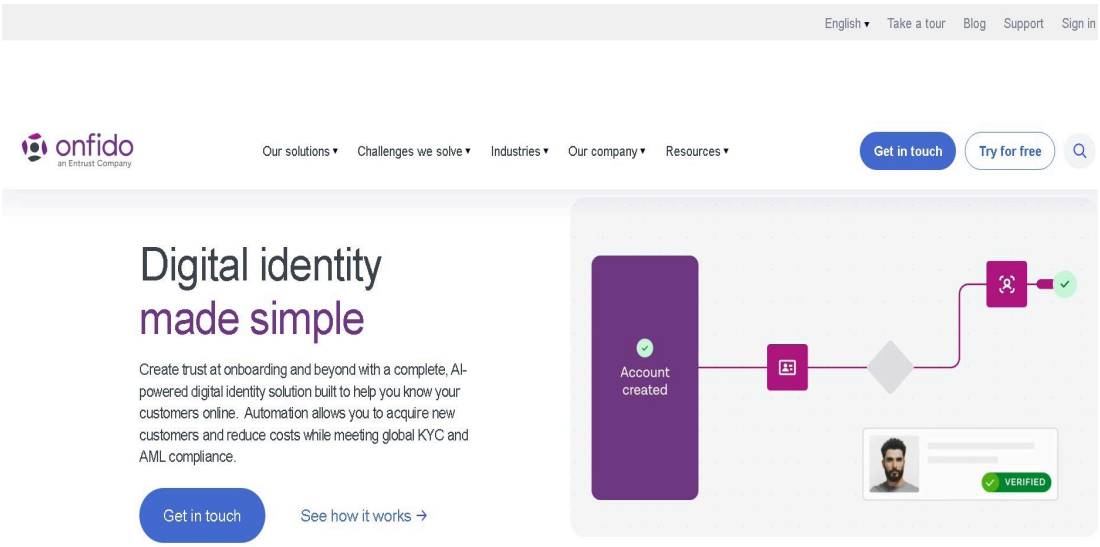

Figure 1.5 : Page d'accueil de « Onfido »

• Processus d'utilisation :

- Les utilisateurs téléchargent une photo de leur pièce d'identité et une selfie via l'application Onfido.
- L'IA compare la photo de la pièce d'identité avec la selfie pour vérifier l'identité.
- L'IA compare la photo de la pièce d'identité avec la selfie pour vérifier l'identité.

• Acteurs :

- Onfido :L'entreprise qui développe et maintient la plateforme.
- Entreprises partenaires : Les entreprises qui utilisent Onfido pour vérifier l'identité de leurs clients.
- Utilisateurs finaux : Les clients qui doivent vérifier leur identité pour accéder aux services.

• Points forts :

- Utilisation de l'IA pour une vérification rapide et précise.
- Convivialité pour les utilisateurs finaux.

• Points faibles :

- Limité aux entreprises privées, ne couvre pas les besoins gouvernementaux.
- Dépendance à la qualité des photos fournies par les utilisateurs.

2.1.4 Serpro (Brésil)

Serpro (Service fédéral de traitement des données) est une entreprise publique brésilienne qui fournit des services de gestion des identités numériques pour le gouvernement. Elle est responsable de la gestion du CPF (Cadastro de Pessoas Físicas) et propose des solutions de vérification d'identité pour les services publics.

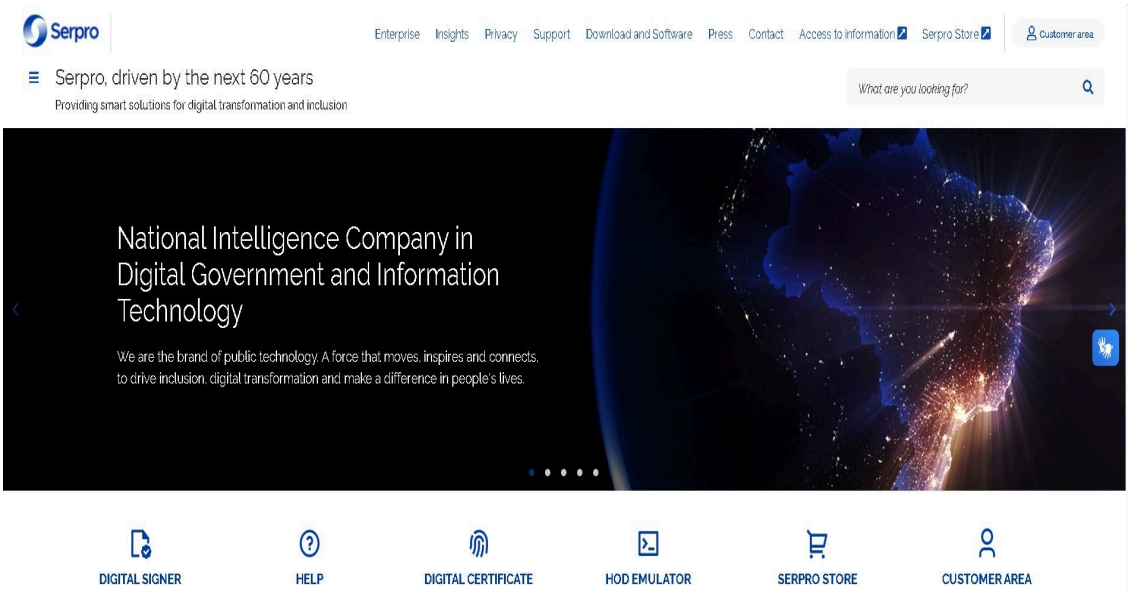

Figure 1.6 : Page d'accueil de « Serpro »

• Processus d'utilisation :

- Les citoyens brésiliens obtiennent un CPF, qui sert d'identifiant unique pour accéder aux services gouvernementaux.
- La plateforme permet de vérifier l'identité des citoyens via des bases de données centralisées.
- Les institutions gouvernementales peuvent accéder aux données pour vérifier l'identité des utilisateurs.

• Acteurs :

- Serpro : L'entreprise publique qui gère la plateforme.
- Gouvernement brésilien : Les institutions publiques qui utilisent la solution pour vérifier l'identité des citoyens.

- Citoyens brésiliens : Les utilisateurs finaux qui utilisent leur CPF pour accéder aux services.

• Points forts :

- Large couverture des services gouvernementaux.
- Intégration avec les systèmes publics existants.

• Points faibles :

- Centralisation des données, ce qui peut poser des problèmes de sécurité.
- Manque de fonctionnalités avancées de détection de fraude en temps réel.

2.2 Critiques des solutions existantes

afin d'évaluer les solutions présentées dans la section précédente, nous avons défini un ensemble de critères axés sur les aspects fonctionnels et non fonctionnels de chaque plateforme. Ces critères visent à mettre en lumière les points forts et les faiblesses de chaque solution. Les critères sont les suivants :

Critère 1 : « Portée géographique »
Évalue la capacité de la solution à être déployée et utilisée dans différentes régions ou pays. Une portée géographique étendue indique une adaptabilité à divers contextes légaux et culturels.
Critère 2 : « Secteur d'application »
Examine les domaines d'utilisation de la solution, tels que les services gouvernementaux, les secteurs bancaires ou les entreprises privées. Ce critère permet de déterminer si la solution répond aux besoins spécifiques de l'utilisateur.
Critère 3 : « Technologies utilisées »
Évalue les technologies mises en œuvre par la solution, telles que la biométrie, l'intelligence artificielle ou les systèmes de stockage décentralisés. Ce critère permet de mesurer l'innovation et l'efficacité de la solution.
Critère 4 : « Sécurité des données »
Analyse la manière dont les données sont stockées et protégées. Une sécurité renforcée, comme la décentralisation des données, réduit les risques de piratage et de fraude.
Critère 5 : « Convivialité pour l'utilisateur »
Évalue la facilité d'utilisation de la solution pour les utilisateurs finaux. Une interface intuitive et simple améliore l'adoption et la satisfaction des utilisateurs.
Critère 6 : « Intégration avec les systèmes existants »
Examine la capacité de la solution à s'intégrer facilement avec les infrastructures et

systèmes déjà en place. Une intégration fluide réduit les coûts et les délais de mise en œuvre.

Critère 7 : « Détection de fraude en temps réel »

Évalue la capacité de la solution à identifier et à prévenir les fraudes en temps réel grâce à des technologies avancées comme l'IA ou la biométrie.

Critère 8 : « Coût de mise en œuvre »

Analyse les coûts associés à l'adoption et à la mise en œuvre de la solution. Ce critère est crucial pour les organisations ayant des budgets limités.

Critère 9 : « Couverture des services »

Évalue l'étendue des services offerts par la solution, tels que l'accès aux services gouvernementaux, la vérification d'identité ou la gestion des identifiants uniques.

Tableau 1.1 : Analyse des solutions existantes

Critères de comparaison	e-Estonia (Estonie)	IDEMIA (Solution Globale)	Onfido (Royaume-Uni)	Serpro (Brésil)
1. Portée géographique	Limitée à l'Estonie	Plus de 180 pays	Principalement Europe et Amérique du Nord	Limitée au Brésil
2. Secteur d'application	Gouvernement et services publics	Secteurs bancaires et gouvernementaux	Entreprises privées	Gouvernement et services publics
3. Technologies utilisées	Carte d'identité numérique, signature électronique	Reconnaissance faciale, empreintes digitales, iris	Reconnaissance faciale, IA, vérification de documents	Bases de données centralisées, vérification d'identité
4. Sécurité des données	Décentralisée (haute sécurité)	Base de données sécurisée	Stockage sécurisé des données	Centralisée (risques de sécurité)
5. Convivialité pour l'utilisateur	Interface simple pour les citoyens	Complexe pour les utilisateurs finaux	Très conviviale	Interface basique
6. Intégration avec les systèmes existants	Difficile à adapter à d'autres pays	Complexe et coûteuse	Facile via des API	Intégration avec les systèmes publics

7. Détection de fraude en temps réel	Non	Oui (technologies biométriques avancées)	Oui (via IA)	Non
8. Coût de mise en œuvre	Élevé (infrastructure gouvernementale)	Très élevé	Modéré	Faible (géré par le gouvernement)
9. Couverture des services	Large éventail de services publics	Services bancaires et gouvernementaux	Services privés (banques, assurances, etc.)	Services gouvernementaux

3. Solution proposée

Identity Secure vise à combler les lacunes des systèmes existants au Brésil en intégrant des technologies biométriques avancées, une architecture décentralisée, et des fonctionnalités de détection de fraude en temps réel. En s'appuyant sur des API biométriques et des technologies cloud, Identity Secure offre une solution innovante pour sécuriser les identifiants fiscaux et prévenir les fraudes.

Renforcement de la confiance et de la crédibilité : En sécurisant les échanges et en garantissant l'intégrité des identifiants fiscaux, la solution inspire confiance tant aux utilisateurs qu'aux institutions partenaires, en phase avec les exigences formulées lors de l'analyse des besoins.
Optimisation de l'expérience utilisateur : La simplification des processus par une interface intuitive et l'automatisation des tâches permet de réduire les erreurs humaines et d'améliorer l'accessibilité, répondant ainsi aux lacunes relevées dans les systèmes traditionnels.
Adaptabilité aux évolutions du marché : Conçue selon une architecture modulaire, Identity Secure peut évoluer en fonction des nouvelles normes et technologies, assurant sa pertinence à long terme.
Réduction des coûts et amélioration de l'efficacité opérationnelle : La digitalisation et la centralisation des processus de vérification permettent de minimiser les coûts liés aux interventions manuelles et de renforcer l'efficacité globale du système.
Vision globale et approche intégrée : En offrant une vue unifiée de la gestion des identités, la solution crée un écosystème harmonieux reliant utilisateurs finaux, institutions et technologies, ce qui constitue un avantage concurrentiel majeur.

4. Spécification des besoins

Dans cette section, nous mettons en lumière les différents intervenants impliqués dans le fonctionnement de notre application, ainsi que leurs responsabilités respectives. En outre, nous décrivons les exigences fonctionnelles et non fonctionnelles auxquelles notre application vise à répondre.

4.1. Identification des acteurs

Dans notre application, nous identifions cinq acteurs, correspondant chacun à un rôle joué par une personne physique ou un élément système interagissant directement avec le système :
- **Internaute** : Il s'agit d'une personne non authentifiée par la plateforme et désirant consulter les informations et les services proposés par la plateforme.
- **citoyens brésiliens** : Personne physique qui est à la demande d'un cpf ou peut gérer son statut tout en le consultant.
- **Manager CPF** : Responsable de la gestion de la plateforme secure identity au niveau organisationnel. Il supervise les comptes CPF, crée et gère les comptes des officier de polices et suivre les statuts de leurs CPF .
- **ChatBot** : Module intelligent fournissant une assistance automatisée aux utilisateurs. Il peut aider à la navigation dans l'application et réponds aux questions sur les processus d'audit.

4.2. Spécifications des besoins fonctionnels

Les spécifications fonctionnelles détaillent les différentes fonctionnalités de l'application et délimitent son champ d'action dans le projet. Elles découlent des besoins exprimés par le client. Ainsi, notre application doit satisfaire les exigences spécifiques de chaque utilisateur et doit répondre aux exigences suivantes pour chaque acteur.

4.2.1 Besoins fonctionnels de l'acteur « Internaute »

Le tableau 1 illustre les différents besoins fonctionnels de l'acteur « Internaute ».

Tableau 1.2 : Besoins fonctionnels de l'acteur « Internaute »

Fonctionnalité	Description
S'informer	L'internaute peut consulter les différentes fonctionnalités et services intégrés dans identity-secure sans besoin de s'inscrire ou de se connecter.
S'inscrire	L'internaute peut accéder à la page d'inscription pour devenir un utilisateur enregistré sur la plateforme identity-secure.

4.2.2 Besoins fonctionnels de l'acteur «citoyens brésiliens»

Le tableau 1 illustre les différents besoins fonctionnels de l'acteur «citoyens brésiliens».

Tableau 1.3 : Besoins fonctionnels de l'acteur « citoyens brésiliens »

Fonctionnalité	Description
Remplir formulaire	Le citoyen brésilien peut créer un compte pour prendre rendez vous avec l'officier de police afin de fournir ses données biométriques .
S'authentifier	Le citoyen brésilien peut s'authentifier sur la plateforme identity-secure en utilisant son adresse e-mail et son mot de passe afin d'accéder à ses fonctionnalités et données personnelles.
Récupérer Mot de passe	En cas d'oubli de son mot de passe, Le citoyens brésiliens a la possibilité de récupérer son mot de passe via un processus sécurisé de réinitialisation de mot de passe.
Consulter l'historique des usages du cpf	Le citoyen brésilien peut consulter un historique détaillé des activités associées à son CPF
Déclarer une demande de blocage en cas de vol/fraude/usurpation	En cas de vol, fraude ou usurpation d'identité, le citoyen brésilien peut soumettre une demande de blocage de son CPF via la plateforme.
Créer un compte bancaire virtuel	Le citoyen brésilien peut ouvrir un compte bancaire virtuel directement via Identity-Secure pour faciliter ses transactions financières sécurisées.

4.2.3 Besoins fonctionnels de l'acteur « Manager CPF»

Le tableau 1.4 montre les différents besoins fonctionnels de l'acteur «Manager CPF »

Tableau 1.4 : Besoins fonctionnels de l'acteur « Manager CPF »

Fonctionnalité	**Description**
S'authentifier	Le Manager peut s'authentifier sur la plateforme identity-secure en utilisant son adresse e-mail et son mot de passe afin d'accéder à ses fonctionnalités et données personnelles.
detecter les fraudes	en appliquant l'algorithme de déduplication pour le nouvel compte enregistré , le manager peut détecter les fraudes.
envoi des notifs	Le Manager peut envoyer des notifications à la personne qui détient ce CPF.
Controler le statut des CPF	Le Manager peut arreter , activer, suspendre , bloquer un CPF.
Remplir la blacklist	Le Manager peut mettre les personnes ayant des cpf suspendu dans une blacklist.
activer/désactiver les comptes CPF	Le Manager peut activer / désactiver les comptes CPF.Le Manager peut activer / désactiver les comptes CPF.

4.2.4 Besoins fonctionnels de l'acteur «officier de police»

Le tableau 1.5 illustre les différents besoins fonctionnels de l'acteur «officier de police».

Tableau 1.5 : Besoins fonctionnels de l'acteur « officier de police »

Fonctionnalité	Description
S'authentifier	L'officier de police peut s'authentifier sur la plateforme identity-secure en utilisant son adresse e-mail et son mot de passe pour accéder à ses fonctionnalités et données personnelles.
Récupérer Mot de passe	En cas d'oubli de son mot de passe, l'Manager Banque a la possibilité de récupérer son mot de passe via un processus sécurisé de réinitialisation de mot de passe.
Téléverser les données biométriques	L'officier de police peut téléverser les données biométriques des v=citoyens pour qu'il détiennent leur numéro CPF.
Envoyer mail de check-up	L'officier de police à la possibilité d'envoyer des mails aux citoyens ayant rempli des formulaires mais qui n'ont pas assister au rendez-vous.
Rapporter les usurpateur	L'officier de police peut rapporter les personnes qui ont déjà un cpf .

4.2.5 Besoins fonctionnels de l'acteur « ChatBot»

Le tableau 1.6 illustre les différents besoins fonctionnels de l'acteur «ChatBot».

Tableau 1.6 : Besoins fonctionnels de l'acteur « ChatBot »

Fonctionnalité	Description
Procurer Aide	Le ChatBot peut fournir une assistance automatisée aux managers et aux citoyens ayant des comptes CPF en répondant à leurs questions fréquemment posées et en leur fournissant des informations pertinentes sur l'application et les processus d'audit.

4.3 Spécifications des besoins non fonctionnels

Dans le cadre du projet identity-secure, plusieurs besoins non fonctionnels revêtent une importance capitale pour garantir la fiabilité et la qualité du système. Ces exigences sont essentielles pour assurer un fonctionnement optimal de l'application. Voici les principaux besoins non fonctionnels à prendre en considération :

- **Sécurité** : L'application identity-secure doit garantir la sécurité des informations en limitant l'accès aux données sensibles uniquement aux utilisateurs autorisés. L'accès à certains modules de l'application doit être protégé par des mécanismes d'authentification, tels que le login et le mot de passe.
- **Performance du système** : Garantir des temps de réponse rapides et des performances optimales de l'application, même lorsqu'elle est soumise à des charges élevées ou à un grand nombre d'utilisateurs simultanés.
- **Évolutivité** : Concevoir l'architecture de l'application de manière à ce qu'elle puisse facilement évoluer et s'adapter à de nouvelles exigences fonctionnelles et à une augmentation de la charge de travail sans compromettre les performances.
- **Fiabilité** : Assurer la stabilité et la disponibilité de l'application en minimisant les temps d'arrêt et en mettant en place des mécanismes de sauvegarde et de récupération en cas de défaillance du système.
- **Compatibilité multiplateforme** : Assurer la compatibilité de l'application avec différents navigateurs web, systèmes d'exploitation et appareils mobiles pour offrir une expérience utilisateur homogène sur différentes plateformes.
- **Accessibilité** : Garantir que l'application est accessible à tous les utilisateurs, y compris ceux ayant des besoins spécifiques en matière d'accessibilité, en se conformant aux normes et directives d'accessibilité web.

5. Méthodologie adoptée

Une méthodologie est un cadre utilisé pour structurer, planifier et contrôler le développement d'une application. Dans la réalisation de notre projet, nous avons adopté «Scrum» comme méthodologie de conception et de développement.

Scrum est une méthodologie de gestion de projet agile. Elle met l'accent sur la collaboration, la livraison continue de logiciels fonctionnels et l'adaptabilité aux changements. En favorisant les interactions entre les individus, la réactivité aux besoins changeants des clients et la simplification des processus, Scrum permet aux équipes de travailler de manière efficace et productive. Ses piliers de transparence, de vérification et d'adaptation garantissent une approche itérative et incrémentale, permettant une amélioration continue du produit et du processus de développement. Pour notre projet identity-secure, où la communication transparente et la livraison régulière de

fonctionnalités sont essentielles, Scrum offre un cadre idéal pour gérer efficacement la complexité et l'évolution des besoins.

Dans une équipe Scrum, 3 rôles sont définis à savoir :
Le product owner : C'est le responsable du produit qui représente le client, il porte la vision du produit à réaliser.
Le Scrum master : Il 'est un membre de l'équipe, il a le rôle d'aider l'équipe à avancer de manière autonome.
Le Scrum Team : La particularité d'une équipe Scrum qu'elle est dépourvue de toute hiérarchie interne. Une équipe Scrum est auto-organisée.
Le cycle de vie de la méthode Scrum se décompose en plusieurs Sprint successifs, la figure suivante présente le processus de développement d'un projet selon Scrum :

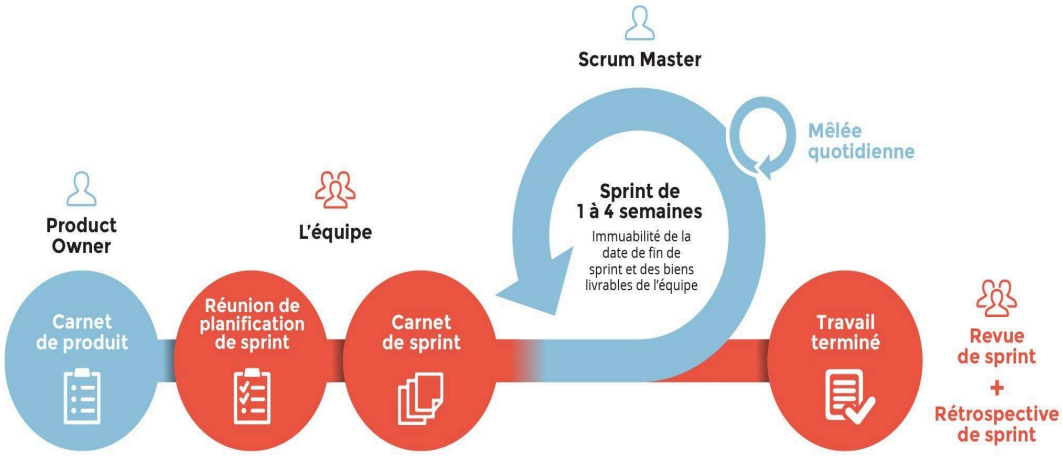

Figure 1.7 : Processus de Scrum

La figure 1.6 illustre le principe de base de la méthodologie Scrum. Elle définit certains mots clés qui nous serviront tout au long du projet et de la rédaction du présent mémoire.

- **Carnet de produit (Product Backlog) :** liste des fonctionnalités attendues d'un produit. Il est élaboré avant le lancement des sprints, dans la phase de préparation. Il est utilisé pour planifier une « release » et au cours d'une réunion de planification d'un sprint afin de décider du sous-ensemble qui sera réalisé.
- **Réunion de planification de sprint (Sprint Planning Meeting) :** réunion pour planifier le sprint à traiter après avoir fixé son cadre.
- **Carnet de sprint (Sprint Backlog) :** liste des tâches à implémenter dans un sprint classé par priorité et état.
- **Mêlée quotidienne (Scrum Meeting) :** c'est une réunion de durée 5 minutes organisée quotidiennement.

- **Revue de sprint (Burn-Down Chart) :** c'est une activité réalisée à la fin de chaque sprint. Il s'agit d'une réunion durant laquelle l'équipe de projet présente le travail réalisé pour l'évaluer et le valider.
- **Rétrospective de sprint (Sprint Rétrospective) :** c'est une activité réalisée à la fin de chaque sprint. Il s'agit d'une réunion durant laquelle l'équipe de projet présente le travail réalisé pour l'évaluer et le valider.

Conclusion

Dans ce premier chapitre introductif, nous avons situé notre projet **identity-secure** dans son contexte général et exposé succinctement les objectifs visés. Ainsi nous avons examiné les solutions existantes, mis en évidence leurs limitations et proposé une alternative. Ensuite, nous avons identifié les divers acteurs impliqués dans le projet, ainsi que les exigences fonctionnelles et non fonctionnelles. Enfin, nous avons détaillé la méthodologie Scrum que nous avons sélectionnée pour piloter le projet "identity-secure". Le chapitre suivant se concentrera sur la phase de préparation.