Identity Secure

Cahier de Charge

Table des matières

1. Introduction

1.1. Contexte Général

Identity Secure est une application web innovante conçue pour générer une identité numérique unique pour les citoyens, en particulier au Brésil. Elle repose sur des données biométriques telles que le visage, l'iris et les empreintes digitales pour créer un CPF (Cadastro de Pessoas Físicas) sécurisé. L'application permet de prévenir les fraudes liées aux activités financières, comme la création de comptes bancaires. Chaque citoyen disposant d'un CPF reçoit des notifications automatiques pour toute utilisation dans des transactions financières. Identity Secure intègre également un chatbot intelligent pour assister les citoyens dans les demandes de vérification, les alertes de sécurité et les procédures de récupération en cas de fraude.

1.2. Contexte et Enjeux du Projet

Le projet s'inscrit dans un contexte où la gestion des identifiants fiscaux, appelés CPF (Cadastro de Pessoas Físicas), est cruciale pour prévenir les fraudes et garantir l'intégrité des systèmes financiers et sociaux. Caixa, l'une des plus grandes banques du Brésil, fait face à des fraudes massives impliquant des CPF

multiples ou usurpés pour bénéficier illégalement des aides sociales ou effectuer des transactions frauduleuses.

Le CPF (Cadastro de Pessoas Físicas)

Le CPF est l'identifiant fiscal des personnes physiques au Brésil, équivalent au numéro de sécurité sociale (NSS) aux États-Unis ou au numéro d'identification fiscale (NIF) en France. Il est attribué par la Receita Federal do Brasil.

Caractéristiques du CPF

- Numéro unique à 11 chiffres.
- Obligatoire pour toute transaction financière.
- Délivré également aux étrangers ayant des obligations fiscales au Brésil.

Types de Fraudes Liées au CPF

- **Usurpation d'identité et CPF multiples** : Création de faux CPF pour percevoir plusieurs aides sociales.
- **Faux retraités** : Perception de retraites pour des personnes décédées.
- **Fraude aux allocations chômage** : Perception d'allocations chômage en parallèle de pensions de retraite.
- **Blanchiment de CPF** : Utilisation de CPF de personnes vulnérables pour des activités illégales.

Mesures de Lutte Contre les Fraudes

- Croisement des bases de données fiscales et sociales.
- Reconnaissance biométrique obligatoire.
- Contrôles stricts des paiements liés aux registres de décès.

1.3. Présentation de Twyn-T4ISB

Twyn-T4ISB est une entreprise innovante spécialisée dans les technologies de biométrie, blockchain et développement logiciel. Elle accompagne les entreprises dans leur transformation digitale grâce à des solutions basées sur l'innovation, la technologie et la simplicité. Forte de son expertise en intégration biométrique et

en solutions d'identification, Twyn-T4ISB développe des plateformes de gestion d'identité basées sur une architecture microservices et des technologies cloud.

Le projet s'inscrit dans cette dynamique en intégrant une API biométrique pour la détection et la suppression des doublons d'images faciales dans les bases de données, contribuant ainsi à l'amélioration de la sécurité des systèmes d'identité.

2. Analyse du Marché et de l'Existant

2.1. 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 :

1. **e-Estonia (Estonie)** : Plateforme numérique utilisée en Estonie pour la gestion des identités numériques des citoyens, basée sur une carte d'identité numérique et une signature électronique.
2. **IDEMIA (Solution Globale)** : Entreprise spécialisée dans les technologies d'identification biométrique, présente dans plus de 180 pays, offrant des solutions basées sur la reconnaissance faciale, les empreintes digitales et l'iris.
3. **Onfido (Royaume-Uni)** : Plateforme de vérification d'identité basée sur l'intelligence artificielle, utilisant la reconnaissance faciale et la vérification de documents pour authentifier les utilisateurs.
4. **Serpro (Brésil)** : Entreprise publique brésilienne fournissant des services de gestion des identités numériques pour le gouvernement, responsable de la gestion du CPF.

2.2. Limites des Solutions Actuelles

Les solutions existantes présentent plusieurs limitations :

- **Portée géographique limitée** : Certaines solutions sont conçues pour des marchés spécifiques et sont difficiles à adapter à d'autres contextes nationaux.

- **Sécurité des données** : Les systèmes centralisés comme Serpro présentent des risques de sécurité accrus.
- **Intégration complexe** : Solutions comme IDEMIA nécessitent une intégration complexe et coûteuse avec les systèmes existants.
- **Détection de fraude limitée** : Certaines solutions manquent de fonctionnalités avancées de détection de fraude en temps réel.
- **Coûts élevés** : Mise en œuvre souvent onéreuse, notamment pour les solutions globales comme IDEMIA.
- **Dépendance technologique** : Solutions parfois dépendantes de la qualité des données fournies par les utilisateurs.

3. Présentation de la Solution

3.1. Description Générale

Identity Secure est une application web innovante qui vise à révolutionner la gestion de l'identité numérique au Brésil en créant un système sécurisé de génération et de gestion des CPF. La solution est conçue pour répondre aux défis actuels de fraude et d'usurpation d'identité, tout en offrant une expérience utilisateur fluide et intuitive.

3.2. Avantages de la Solution

Identity Secure vise à combler les lacunes des systèmes existants au Brésil en offrant les avantages suivants:

- **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.
- **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.
- **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.
- **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.

3.3. Fonctionnalités Principales

- Génération d'un CPF unique pour chaque citoyen, attribué une seule fois dans une vie.
- Association du CPF aux données biométriques (visage, empreintes digitales, iris).
- Suivi des transactions bancaires, achats en ligne et autres opérations financières.
- Alertes automatiques pour les activités suspectes ou les tentatives de fraude.
- Assistance utilisateur via chatbot pour la vérification et la gestion des alertes.
- Déduplication biométrique pour prévenir les identités multiples.

4. Acteurs du Système

4.1. Internaute

Définition : Personne non authentifiée par la plateforme qui souhaite consulter les informations et les services proposés par Identity Secure.

Caractéristiques :

- N'a pas de compte sur la plateforme
- Accès limité aux informations générales
- Peut s'inscrire pour devenir un utilisateur enregistré

Objectifs :

- S'informer sur les services d'Identity Secure
- Comprendre le fonctionnement du système CPF

- S'inscrire pour accéder aux fonctionnalités complètes

4.2. Citoyen Brésilien

Définition : Personne physique qui demande un CPF ou qui gère son CPF existant via la plateforme.

Caractéristiques :

- Possède ou souhaite obtenir un CPF
- Doit s'authentifier pour accéder à ses données personnelles
- Peut recevoir des notifications concernant l'utilisation de son CPF

Objectifs :

- Obtenir un CPF sécurisé
- Surveiller l'utilisation de son identifiant fiscal
- Protéger son identité contre les fraudes
- Gérer ses transactions financières en toute sécurité
- Signaler rapidement les activités frauduleuses

Interactions avec le système :

- Inscription et authentification
- Prise de rendez-vous avec l'officier de police
- Fourniture de données biométriques
- Consultation de l'historique d'utilisation du CPF
- Déclaration de fraude et demande de blocage
- Création de compte bancaire virtuel

4.3. CPF Manager

Définition : Responsable de la gestion organisationnelle de la plateforme Identity Secure.

Caractéristiques :

- Employé autorisé avec des droits d'administration

- Accès à des fonctionnalités avancées de gestion et de supervision
- Responsable de la sécurité et de l'intégrité du système

Objectifs :

- Assurer la sécurité et l'intégrité du système CPF
- Prévenir et détecter les fraudes
- Contrôler les statuts des CPF
- Gérer les comptes des officiers de police

Interactions avec le système :

- Authentification avec privilèges d'administration
- Application d'algorithmes de déduplication pour détecter les fraudes
- Envoi de notifications aux utilisateurs
- Contrôle des statuts des CPF (activation, désactivation, suspension, blocage)
- Gestion de la liste noire des utilisateurs frauduleux
- Supervision des activités des officiers de police

4.4. Officier de Police

Définition : Agent de police responsable de la vérification physique des identités et de la collecte des données biométriques.

Caractéristiques :

- Représentant officiel des forces de l'ordre
- Accès sécurisé à des fonctionnalités spécifiques du système
- Intervient dans le processus de validation de l'identité

Objectifs :

- Vérifier l'identité physique des demandeurs de CPF
- Collecter les données biométriques de manière sécurisée
- Prévenir les fraudes à l'identité
- Contribuer à l'intégrité du système CPF

Interactions avec le système :

- Authentification sur la plateforme
- Validation des demandes de génération de CPF
- Téléchargement des données biométriques collectées
- Envoi de rappels aux citoyens qui n'ont pas assisté au rendez-vous
- Signalement des tentatives d'usurpation d'identité
- Coordination avec le CPF Manager pour les cas suspects

4.5. ChatBot

Définition : Module intelligent intégré qui fournit une assistance automatisée aux utilisateurs de la plateforme.

Caractéristiques :

- Disponibilité 24/7
- Répond aux questions fréquentes
- Capable de guider les utilisateurs dans leurs démarches

Objectifs :

- Améliorer l'expérience utilisateur
- Réduire la charge de travail du support client humain
- Fournir des informations rapides et précises

Interactions avec le système :

- Fourniture d'aide et d'informations aux utilisateurs
- Assistance pour la navigation dans l'application
- Réponse aux questions sur les processus d'identification et de sécurité
- Orientation vers les ressources appropriées

5. Exigences Fonctionnelles Détaillées

5.1. Exigences pour l'Internaute

Code	Fonctionnalité	Description	Priorité
INT-01	S'informer	L'internaute peut consulter les différentes fonctionnalités et services intégrés dans Identity Secure sans besoin de s'inscrire ou de se connecter.	Haute
INT-02	S'inscrire	L'internaute peut accéder à la page d'inscription pour devenir un utilisateur enregistré sur la plateforme Identity Secure.	Haute
INT-03	Consulter la FAQ	L'internaute peut accéder à une section de questions fréquemment posées pour mieux comprendre le fonctionnement du système.	Moyenne
INT-04	Contacter le support	L'internaute peut envoyer des messages au support technique en cas de questions ou de problèmes.	Moyenne

5.2. Exigences pour le Citoyen Brésilien

Code	Fonctionnalité	Description	Priorité
CIT-01	Remplir formulaire	Le citoyen brésilien peut créer un compte pour prendre rendez-vous avec l'officier de police afin de fournir ses données biométriques.	Haute
CIT-02	S'authentifier	Le citoyen brésilien 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.	Haute
CIT-03	Récupérer mot de passe	En cas d'oubli de son mot de passe, le citoyen brésilien a la possibilité de récupérer son mot de passe via un processus sécurisé de réinitialisation.	Haute

CIT-04	Consulter l'historique des usages du CPF	Le citoyen brésilien peut consulter un historique détaillé des activités associées à son CPF.	Haute
CIT-05	Déclarer une demande de blocage	En cas de vol, fraude ou usurpation d'identité, le citoyen brésilien peut soumettre une demande de blocage de son CPF via la plateforme.	Haute
CIT-06	Créer un compte bancaire virtuel	Le citoyen brésilien peut ouvrir un compte bancaire virtuel directement via Identity Secure pour faciliter ses transactions financières sécurisées.	Moyenne
CIT-07	Modifier ses informations personnelles	Le citoyen peut mettre à jour ses coordonnées et autres informations non biométriques.	Moyenne
CIT-08	Recevoir des notifications	Le citoyen reçoit des alertes en temps réel pour toute utilisation de son CPF.	Haute

5.3. Exigences pour le CPF Manager

Code	Fonctionnalité	Description	Priorité
MNG-01	S'authentifier	Le Manager peut s'authentifier sur la plateforme Identity Secure en utilisant son adresse e-mail et son mot de passe pour accéder à ses fonctionnalités administratives.	Haute
MNG-02	Détecter les fraudes	En appliquant l'algorithme de déduplication pour les nouveaux comptes enregistrés, le manager peut détecter les fraudes potentielles.	Haute
MNG-03	Envoyer des notifications	Le Manager peut envoyer des notifications aux personnes qui détiennent un CPF, notamment en cas d'activité suspecte.	Haute

MNG-04	Contrôler le statut des CPF	Le Manager peut arrêter, activer, suspendre ou bloquer un CPF selon les besoins.	Haute
MNG-05	Gérer la liste noire	Le Manager peut ajouter à une liste noire les personnes ayant des CPF suspendus pour fraude.	Haute
MNG-06	Gérer les comptes des officiers	Le Manager peut créer, modifier et désactiver les comptes des officiers de police.	Moyenne
MNG-07	Générer des rapports	Le Manager peut produire des rapports statistiques sur les fraudes détectées et les activités du système.	Moyenne
MNG-08	Configurer les paramètres système	Le Manager peut ajuster les paramètres de sécurité et de notification du système.	Moyenne

5.4. Exigences pour l'Officier de Police

Code	Fonctionnalité	Description	Priorité
POL-01	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 spécifiques.	Haute
POL-02	Récupérer mot de passe	En cas d'oubli de son mot de passe, l'officier de police a la possibilité de récupérer son mot de passe via un processus sécurisé de réinitialisation.	Haute
POL-03	Téléverser les données biométriques	L'officier de police peut télécharger les données biométriques des citoyens pour qu'ils obtiennent leur numéro CPF.	Haute
POL-04	Envoyer mail de rappel	L'officier de police a la possibilité d'envoyer des mails aux citoyens	Moyenne

		ayant rempli des formulaires mais qui n'ont pas assisté au rendez-vous.	
POL-05	Signaler les usurpateurs	L'officier de police peut signaler les personnes qui tentent d'obtenir un CPF alors qu'elles en possèdent déjà un.	Haute
POL-06	Gérer les rendez-vous	L'officier de police peut consulter et organiser son calendrier de rendez-vous avec les citoyens.	Moyenne
POL-07	Vérifier les antécédents	L'officier peut consulter une base de données pour vérifier les antécédents des demandeurs.	Moyenne

5.5. Exigences pour le ChatBot

Code	Fonctionnalité	Description	Priorité
BOT-01	Fournir de l'aide	Le ChatBot peut fournir une assistance automatisée aux managers et aux citoyens ayant des comptes CPF en répondant à leurs questions fréquemment posées.	Haute
BOT-02	Guider les utilisateurs	Le ChatBot peut guider les utilisateurs à travers les différentes fonctionnalités de la plateforme.	Moyenne
BOT-03	Escalader les problèmes	Le ChatBot peut transférer les conversations à un agent humain lorsque les questions sont trop complexes.	Moyenne
BOT-04	Fournir des mises à jour	Le ChatBot peut informer les utilisateurs des mises à jour du système et des nouvelles fonctionnalités.	Basse

6. Exigences Non Fonctionnelles

6.1. Sécurité

- **ENF-01** : L'application doit implémenter un mécanisme d'authentification robuste pour protéger l'accès aux données sensibles.
- **ENF-02** : Toutes les données personnelles et biométriques doivent être cryptées en utilisant des algorithmes de cryptage standards de l'industrie.
- **ENF-03** : Le système doit être conforme aux réglementations brésiliennes en matière de protection des données personnelles.
- **ENF-04** : Un système de journalisation doit enregistrer toutes les activités critiques pour permettre un audit en cas de besoin.

6.2. Performance

- **ENF-05** : Le système doit pouvoir traiter au moins 1000 demandes simultanées sans dégradation notable des performances.
- **ENF-06** : Le temps de réponse pour les opérations courantes ne doit pas dépasser 2 secondes dans des conditions normales.
- **ENF-07** : La vérification biométrique doit être complétée en moins de 5 secondes.

6.3. Évolutivité

- **ENF-08** : L'architecture doit être modulaire pour permettre l'ajout de nouvelles fonctionnalités sans refonte majeure.
- **ENF-09** : Le système doit pouvoir s'adapter à une augmentation du nombre d'utilisateurs de 20% par an.
- **ENF-10** : Les mises à jour du système doivent pouvoir être déployées sans interruption significative du service.

6.4. Fiabilité

- **ENF-11** : Le système doit être disponible 99,9% du temps (temps d'arrêt maximal de 8,76 heures par an).
- **ENF-12** : Des mécanismes de sauvegarde automatique doivent être en place pour prévenir la perte de données.

- **ENF-13** : Le système doit inclure des mécanismes de récupération en cas de défaillance.

6.5. Compatibilité

- **ENF-14** : L'application web doit être compatible avec les navigateurs courants (Chrome, Firefox, Safari, Edge) dans leurs versions récentes.
- **ENF-15** : L'interface utilisateur doit être responsive pour s'adapter aux différents appareils (ordinateurs, tablettes, smartphones).
- **ENF-16** : Le système doit pouvoir s'intégrer avec les principales plateformes bancaires brésiliennes.

6.6. Accessibilité

- **ENF-17** : L'interface utilisateur doit être conforme aux normes d'accessibilité WCAG 2.1 niveau AA.
- **ENF-18** : Le système doit offrir des alternatives textuelles pour les utilisateurs ayant des déficiences visuelles.
- **ENF-19** : L'application doit être utilisable avec un clavier seul pour les utilisateurs à mobilité réduite.

7. Processus de Fonctionnement

7.1. Génération du CPF (Validation Unique & Vérification Policière)

1. L'utilisateur effectue une demande de génération de CPF via la plateforme.
2. Une vérification de doublon est effectuée via l'API de reconnaissance faciale.
3. Si aucun doublon n'est détecté, une demande est envoyée à un officier de police.
4. L'utilisateur prend rendez-vous avec l'officier pour la collecte des données biométriques.
5. Après validation, le CPF unique est attribué et lié définitivement à l'identité biométrique.

7.2. Utilisation du CPF pour les Transactions

1. Le CPF est utilisé pour ouvrir des comptes bancaires, effectuer des achats en ligne ou des opérations administratives.
2. Le système effectue une double vérification :
    - Le CPF Manager vérifie la validité du CPF.
    - Le Dashboard Biométrique compare l'image faciale à l'identité enregistrée.
3. Si les deux vérifications sont validées, la transaction est approuvée ; sinon, une alerte de fraude est déclenchée.

7.3. Détection et Gestion des Fraudes

1. Le système utilise des algorithmes de déduplication biométrique pour détecter les tentatives de création de CPF multiples.
2. En cas de détection d'une activité suspecte, le CPF Manager est alerté et peut prendre des mesures.
3. Le citoyen concerné reçoit une notification en temps réel et peut confirmer ou signaler une fraude.
4. Si une fraude est confirmée, le CPF peut être bloqué temporairement et une enquête est lancée.
5. Les cas graves de fraude sont signalés aux autorités compétentes pour des poursuites judiciaires.

8. Scénarios D'utilisation

8.1. Inscription et Génération de CPF

João, un citoyen brésilien, souhaite obtenir un CPF sécurisé :

1. João crée un compte sur Identity Secure.
2. Le système vérifie l'existence d'un CPF via l'API de comparaison faciale.
3. Si aucune correspondance n'est trouvée, une demande de vérification est envoyée à la police.
4. João reçoit une notification pour prendre rendez-vous avec un officier de police.

5. Lors du rendez-vous, l'officier collecte ses données biométriques (photo du visage, empreintes digitales, scan de l'iris).
6. Après validation par l'officier, le système génère un CPF unique pour João.
7. João reçoit une confirmation par email avec son numéro CPF et les informations d'accès à son compte.

8.2. Utilisation pour une Transaction Bancaire

João souhaite ouvrir un compte bancaire en utilisant son CPF :

1. João se rend à sa banque et fournit son CPF pour ouvrir un compte.
2. La banque transmet le CPF au système Identity Secure pour vérification.
3. Le système valide le CPF et demande à João de se soumettre à une vérification biométrique rapide.
4. Le système compare son visage avec l'image enregistrée dans la base de données.
5. Si les vérifications sont positives, João est autorisé à créer son compte bancaire.
6. João