Ce document et le contenu qui est présenté sont la propriété exclusive de SafeFlat. Ils contiennent des informations confidentielles et sont destinés uniquement à la personne ou l'entité à laquelle ils sont adressés. Toute divulgation, reproduction, distribution ou autre utilisation de ces informations par des personnes ou des entités autres que le destinataire prévu est **interdite**.

Si vous avez reçu cette présentation par erreur, veuillez en informer l'expéditeur immédiatement et supprimer le document original. L'usage non autorisé des informations contenues dans ce document peut vous exposer à des sanctions **civiles et/ou pénales** selon les lois en vigueur.

SafeFlat

Architecture SafeFlat App

Architecture de l’Application

1. Page d’accueil / Landing Page

- Explication concise de l'objectif de l'application, de ses fonctionnalités et de ses avantages. L’idée est de s’inspirer du modèle Revolut, comme une story Instagram, vidéo courte et percutante.

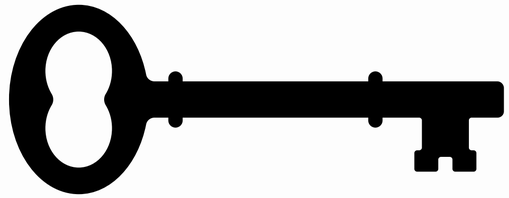
- Éléments visuels ou **infographies** décrivant le processus de **IA Scan** et la protection offerte.

- Appel à l’action, CTA* pour l'inscription ou pour en savoir plus.

Le Call-To-Action, ou CTA, est un bouton situé sur une page web ou dans un e-mail, qui invite le visiteur à effectuer une action. Son objectif est de **convertir les prospects en clients**. Il représente ainsi un véritable outil marketing au service de la conversion.

2. Page d’inscription / Connexion

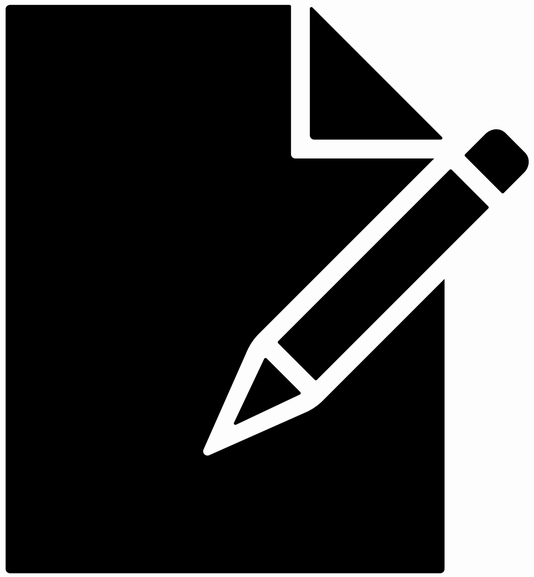
- Formulaires simples pour la création de compte et la connexion, avec validation des champs de saisie.
- Intégration avec OAuth pour permettre aux utilisateurs de s'inscrire ou de se connecter via Facebook ou Google pour plus de commodité.
- Options de mot de passe oublié et de récupération de compte.



OAuth est un protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification, mais de « délégation d'autorisation ».

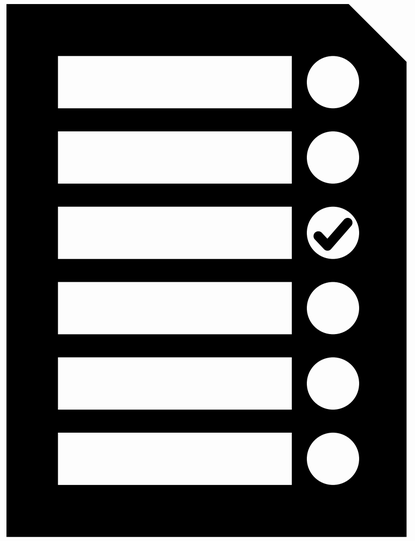
3. Formulaire d’enregistrement de propriété

- Formulaire en plusieurs étapes pour saisir les informations détaillées sur le bien. Surface, étage, nombre de pièces…
- Champs pour télécharger des photos du bien, avec des consignes sur les types de photos requises.
- Validation en temps réel du formulaire pour garantir une saisie de données précise.



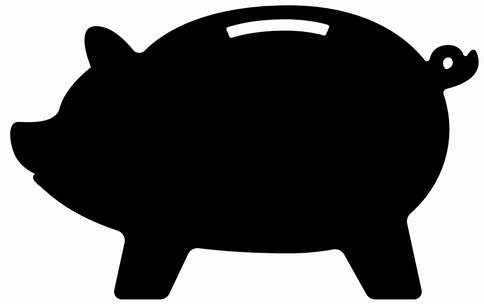
4. Processus de vérification

- Instructions étape par étape pour télécharger des documents d'identité et de propriété.
- Intégration avec des services tiers pour des vérifications en temps réel de l'identité et des documents.



5. Page d’Abonnement

- Plans visuellement distincts avec une comparaison côte à côte des fonctionnalités et des prix.
- Formulaire de paiement sécurisé avec des options pour les cartes de crédit/débit, PayPal, Apple Pay.
- Mentions relatives aux conditions générales d'utilisation et à la politique de confidentialité, ainsi qu'une case d'acceptation des accords de l'utilisateur.



6. Tableau de Bord

- Aperçu des propriétés enregistrées de l'utilisateur avec des vignettes des images de la propriété.
- Résumé des alertes et des notifications, avec une vue détaillée au clic.
- Accès rapide pour changer les plans d'abonnement ou mettre à jour les informations de propriété.

Composants Back-End

Le back-end est responsable du stockage et de la récupération des données à partir de la base de données. Cela inclut la création, la modification et la suppression des données selon les besoins de l'application

1. Gestion des utilisateurs

- Bases de données pour stocker de manière sécurisée les informations d'identification et les profils des utilisateurs, chiffrées pour la sécurité.

- Gestion de session pour maintenir les utilisateurs connectés et gérer les délais d'expiration.

2. Base de données de propriétés

- Schéma de base de données sécurisé et structuré pour stocker les détails des propriétés, les images et les métadonnées.

- Fonctionnalité d'indexation et de recherche pour une récupération rapide et des processus de correspondance.

3. Moteur de Numérisation

- Algorithmes pour numériser et analyser les données à partir des sites Web ciblés, les comparant aux données des propriétés des utilisateurs.

- Service de planification pour des numérisations périodiques en fonction des niveaux d'abonnement.

- Mécanismes de journalisation et d'audit pour enregistrer l'historique des numérisations et les résultats.

4. Système d’Alerte

- Configuration d'un service d'e-mails et de notifications push pour informer les utilisateurs des résultats des numérisations.

- Niveaux d'alerte personnalisables, permettant aux utilisateurs de définir l'urgence et le type d'alertes qu'ils souhaitent recevoir.

5. Gestions des Abonnements

- Intégration avec des passerelles de paiement pour gérer les transactions et les paiements récurrents.
- Système automatisé pour la mise à niveau ou la rétrogradation des plans d'abonnement et la tarification au prorata si nécessaire.
- Alertes automatisées pour les renouvellements d'abonnement et les problèmes de paiement.

6. Facilités de Génération de rapports et d’actions

- Génération de modèles pour la création de notifications formelles en cas de violation de politique.

- Système de suivi de l'état des notifications envoyées aux plateformes ou aux individus publiant des annonces illégales.

7. Modules De Sécurité

- Mise en œuvre de mécanismes d'authentification tels que JWT (JSON Web Tokens) pour un accès API sécurisé.
- Contrôle d'accès basé sur les rôles (RBAC) pour garantir que les utilisateurs disposent des autorisations appropriées au sein de l'application.
- Audits de sécurité réguliers et vérifications de conformité pour respecter les normes légales et de l'industrie.

JWT pour JSON Web Token est une méthode sécurisée d'échange d'informations, décrite par la RFC 7519. L'information est échangée sous la forme d'un jeton signé afin de pouvoir en vérifier la légitimité. Ce jeton est compact et peut être inclus dans une URL sans poser de problème.

Le contrôle d'accès basé sur le rôle (RBAC) est un mécanisme de contrôle d'accès qui définit les rôles et les autorisations de chaque utilisateur. Les rôles sont définis en fonction de caractéristiques telles que l'emplacement, le service, l'ancienneté ou les tâches d'un utilisateur. Les autorisations sont attribuées en fonction de l'accès (ce que l'utilisateur peut voir), des opérations (ce que l'utilisateur peut faire) et des sessions (pendant combien de temps l'utilisateur peut le faire).

APIs et Services Tiers

1. API de Vérification

- Intégration d'API pour la vérification en temps réel de documents et d'identités.
- Conformité aux réglementations KYC (Know Your Customer).

Le KYC, ou Know Your Customer, est la procédure mise en œuvre par les entreprises et les banques pour vérifier l' identité de leurs clients ou d' une personne morale conformément aux réglementations de customer due diligence en vigueur.

2. Passerelle de Paiement

- Gestion sécurisée et conforme des informations financières sensibles.
- Prise en charge de plusieurs devises et calculs fiscaux, le cas échéant.

3. Service de Notification

- Solution évolutive pour l'envoi de notifications en temps réel sur différents appareils.
- Options de personnalisation pour le contenu et le style des notifications.

Infrastructures

L'infrastructure d'application désigne les plateformes logicielles qui facilitent la mise en œuvre d'applications d'entreprise. Il s'agit de l'infrastructure qui existe derrière l'interface utilisateur graphique avec laquelle les utilisateurs d'une application interagissent.

1. Serveurs Web

- Configuration de serveurs évolutifs avec équilibrage de charge pour gérer les pics de trafic.
- Chiffrement SSL/TLS pour des requêtes HTTP sécurisées.

SSL/TLS permet de crypter les communications entre un client et un serveur, principalement entre les navigateurs Web et les sites/applications Web.

2. Serveurs de base de données

- Solutions de stockage fiables et redondantes avec des sauvegardes régulières.
- Optimisation pour des requêtes et des transactions à haute performance.

SSL/TLS permet de crypter les communications entre un client et un serveur, principalement entre les navigateurs Web et les sites/applications Web.

3. Serveurs d’Applications

- Traitement de la logique côté serveur et gestion des demandes.
- Gestion efficace des ressources pour garantir des temps de réponse rapides.

Plus spécifiquement, le serveur d'applications est **le principal composant d'exécution dans toutes les configurations et correspond à l'emplacement d'exécution d'une application**. Le serveur d'applications collabore avec le serveur web pour renvoyer une réponse personnalisée dynamique à une demande d'un client.

4. Réseau de Diffusion de Contenue (CDN)

- Distribution des éléments statiques pour améliorer les temps de chargement à l'échelle mondiale.
- Stratégies de mise en cache pour améliorer l'expérience utilisateur.

Un réseau de diffusion de contenu (CDN) est un réseau de serveurs interconnectés qui accélère le chargement des pages Web pour les applications à forte densité de données. CDN peut signifier content delivery network ou content distribution network.

5. Infrastructure de sécurité

- Déploiement d'un pare-feu d'application Web (WAF) et d'une protection contre les attaques par déni

- Un pare-feu d'applications Web (WAF) est une solution de sécurité qui protège les applications Web contre les attaques courantes en surveillant et en filtrant le trafic, en bloquant le trafic malveillant entrant dans une application Web ou les données non autorisées quittant l'application.

- Une attaque par déni de service distribué (DDoS) cible les sites web et les serveurs en perturbant les services réseau afin d'épuiser les ressources d'une application. Les auteurs de ces attaques inondent un site d'un trafic errant, ce qui entraîne une mauvaise fonctionnalité du site ou le met carrément hors ligne. Ces types d'attaques sont en augmentation.