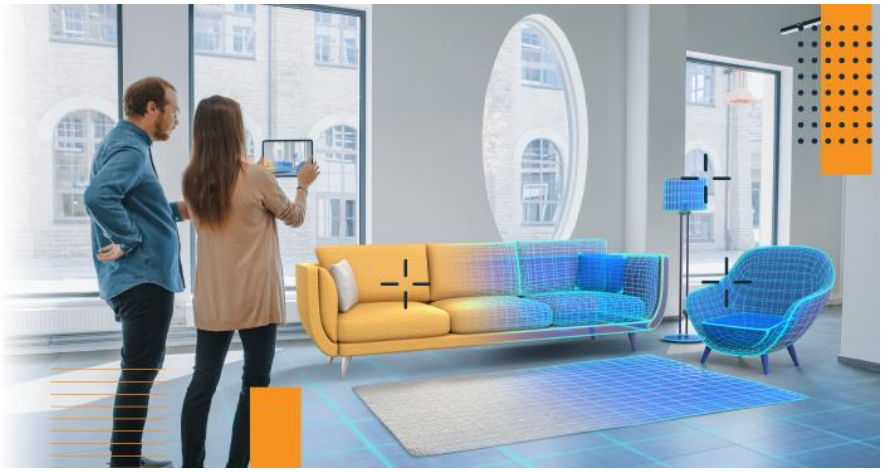
MAISON
EN PLACE



Plan de test

1. Contexte 2
2. Scénarios 3
   2.1 - Fonctionnalité : Authentication 3
   2.2 - Fonctionnalité : Catalogue produit 4
   2.3 - Fonctionnalité : Simulateur de réalité augmentée 5
   2.4 Fonctionnalité : Tunnel d'achat 6

1. Contexte

La plateforme de MaisonEnPlace permet aux utilisateurs de visualiser et d'acheter des meubles via un simulateur de réalité augmentée. Les objectifs de la V2 incluent :

- Améliorer la fiabilité des fonctionnalités critiques.
- Renforcer la sécurité (remplacement des pratiques obsolètes, ex. HTTP, MD5).
- Introduire une méthodologie rigoureuse de tests (BDD).

Nous utiliserons la méthodologie Behavior Driven Development (BDD) pour structurer nos tests, en formulant les scénarios selon le modèle :

- Étant donné que [contexte]
- Quand [action]
- Alors [résultat attendu]

Cette approche garantit que les tests sont centrés sur les comportements attendus, facilitant leur compréhension par toutes les parties prenantes.

2. Scénarios

2.1 - Fonctionnalité : Authentication

Étape	Résultat attendu	Résultat obtenu	Conclusion
Créer un compte avec des informations valides	Compte créé, redirection au catalogue	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Créer un compte avec des informations invalides	Message d'erreur affiché	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Connexion avec des identifiants valides	Connexion réussie, accès au catalogue	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Connexion avec des identifiants invalides	Message d'erreur est affiché	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*

Fonctionnalité exclue :

- **Création de compte via Google ou Apple** : Ces fonctionnalités reposent sur des services tiers (API Google et Apple) qui ne relèvent pas directement de la responsabilité de la plateforme. Les éventuels problèmes ou comportements anormaux liés à ces intégrations doivent être gérés par les fournisseurs des services.

2.2 - Fonctionnalité : Catalogue produit

Étape	Résultat attendu	Résultat obtenu	Conclusion
Afficher la liste complète des produits	Liste complète affichée	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Filtrer les produits par type	Produits filtrés correctement	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Rechercher un produit existant	Produit correspondant affiché	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Rechercher un produit inexistant	Message "Aucun produit trouvé" affiché	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*

2.3 - Fonctionnalité : Simulateur de réalité augmentée

Étape	Résultat attendu	Résultat obtenu	Conclusion
Charger un modèle 3D	Modèle affiché avec succès	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Manipuler le modèle (rotation, zoom)	Manipulations fluides	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Quitter le simulateur	Retour au catalogue	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*

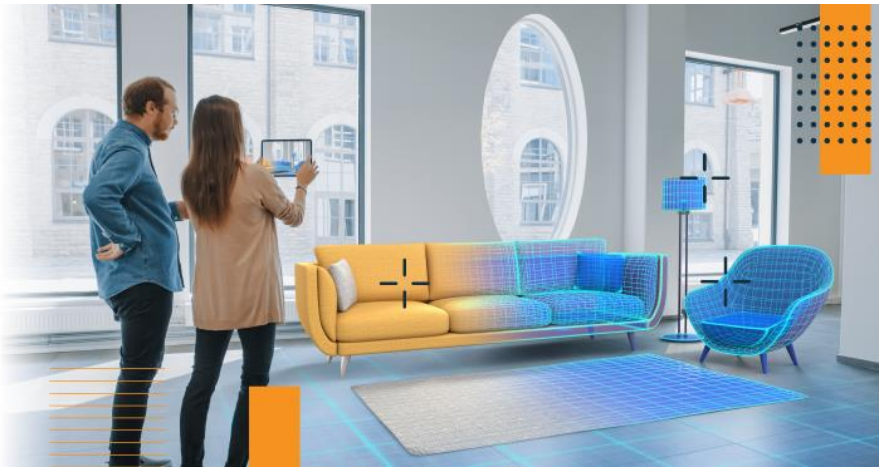
2.4 Fonctionnalité : Tunnel d’achat

Étape	Résultat attendu	Résultat obtenu	Conclusion
Ajouter un produit au panier	Le panier contient le produit	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*
Valider une commande valide	Commande validée et confirmation affichée	*(Laisser vide - devra être rempli par le testeur)*	*(Laisser vide - devra être rempli par le testeur)*

Fonctionnalité exclue :

- **Tests des méthodes de paiement spécifiques (ex. carte bancaire, PayPal)** : Les transactions sont traitées par des prestataires de paiement sécurisés (exemple : Stripe, PayPal). Ces systèmes sont certifiés selon des standards de sécurité élevés (PCI DSS) et ne nécessitent pas de tests internes approfondis sur leur fonctionnement. Nous nous limiterons à vérifier l’intégration générale, comme la redirection vers le fournisseur et le retour avec un statut valide.

MAISON
EN PLACE



Plan de Sécurité

1. Risques et solutions identifiés 2
2. Annexe : Technologies mentionnées..... 4

1. Risques et solutions identifiés

Risque	Contexte	Gravité (de 1 à 5)	Solutions / outils potentiels
Problèmes de compatibilité	L'application peut être incompatible avec certains navigateurs (versions anciennes d'Internet Explorer), appareils (mobiles ou tablettes spécifiques), ou systèmes d'exploitation (versions obsolètes).	**3/5** - Affecte l'expérience utilisateur mais ne bloque pas toutes les fonctionnalités.	**Tester l'application sur plusieurs configurations** : Utiliser des outils comme BrowserStack* pour détecter les incompatibilités. **Utiliser des polyfills** : Ajouter des bibliothèques comme core-js pour garantir la compatibilité avec les versions plus anciennes de JavaScript.
Défaillances des API tierces	Les services externes, comme l'authentification (Google et Apple) ou les paiements, peuvent devenir inaccessibles à cause de pannes ou de changements non anticipés.	**4/5** - Peut bloquer des fonctionnalités clés comme la création de compte ou la finalisation d'achat.	**Logs et alertes :** Intégrer des journaux détaillés et des alertes pour surveiller l'état des API et intervenir rapidement. **Gestion des erreurs robuste :** Notifier les utilisateurs en cas de problème et permettre de réessayer l'action après un délai.
Performances insuffisantes	L'application peut souffrir de lenteurs ou de faible réactivité, particulièrement lors des pics de trafic.	**5** - Dégradation de l'expérience utilisateur, pouvant entraîner des abandons massifs.	**Utilisation de systèmes de cache :** Implémenter Redis* ou un CDN* pour accélérer les temps de réponse. **Optimisation du chargement des pages :** Implémenter le chargement différé (lazy

			loading) et compresser les fichiers.
Vol de données	Une mauvaise sécurisation des données pourrait entraîner leur interception (vol de données personnelles ou bancaires).	**5/5 -** Conséquences graves sur la confiance des utilisateurs et la conformité réglementaire.	**Cryptage des données sensibles :** Assurer des connexions sécurisées avec HTTPS (TLS*). **Stockage sécurisé :** Crypter les données sensibles côté server avec des algorithmes robustes AES*. **Authentification renforcée :** Implémenter OAuth2* et l'authentification multi-facteurs (MFA*).
Pertes de données critiques	Les données critiques (comme les informations utilisateur) pourraient être perdues à cause d'une panne serveur ou d'un mauvais backup.	**4/5 -** Interruption du service et perte de données sensibles.	**Backups automatiques :** Planifier des sauvegardes automatiques sur des serveurs sécurisés. **Plan de reprise :** Prévoir des procédures pour restaurer rapidement le service. **Redondance :** Configurer des bases de données secondaires pour éviter les pertes.
Accès non autorisé aux serveurs	Des attaquants peuvent exploiter des failles pour accéder aux serveurs de l'application.	**5/5 -** Accès aux informations sensibles, compromission de l'ensemble du système.	**Pare-feu et WAF :** Installer un pare-feu applicatif (WAF*) pour bloquer les tentatives malveillantes. **Audits réguliers :** Effectuer des tests de pénétration pour identifier les failles.

			Restrictions d’accès : Configurer des règles strictes (par exemple : accès basé sur les IP ou les rôles).

2. Annexe : Technologies mentionnées

BrowserStack : Outil pour tester les applications sur divers environnements.

Redis : Système de cache rapide pour améliorer les performances.

CDN : Réseau de serveurs pour accélérer la diffusion des contenus.

TLS : Protocole de sécurité pour protéger les communications.

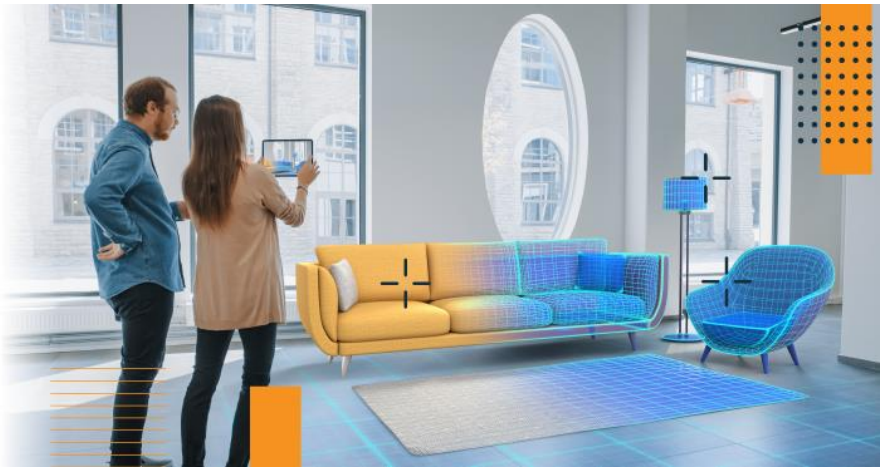
OAuth2 : Standard pour gérer les autorisations d’accès.

AES : Algorithme de cryptage pour sécuriser les données.

MFA : Méthode d’authentification renforcée combinant plusieurs facteurs.

WAF : Pare-feu spécialisé pour protéger les applications web.

MAISON
EN PLACE



Plan de Sauvegarde des Données

1. Définition des besoins 2
   1.1 - Disponibilité et continuité de service 2
   1.2 - Automatisation des sauvegardes 2
   1.3 - Sécurisation des sauvegardes 2
   1.4 - Redondance géographique 2
   1.5 - Tests réguliers de restauration 3
   1.6 - Conformité et traçabilité 3
2. Solution sélectionnée : Solution hybride 4
   2.1 - Avantages 4
   2.2 - Planification des sauvegardes 4
   2.3 - Plan de test de restauration 4
   2.4 - Coûts estimés 5
   2.5 - Rétention des données 5
3. Plan de restauration des données 6

1. Définition des besoins

1.1 - Disponibilité et continuité de service

- **Objectif** :
  Minimiser les interruptions en cas d'incident pour garantir que les utilisateurs puissent acheter des produits à tout moment.

- **Besoins** :
  - Sauvegardes permettant une restauration rapide (RTO* court)
  - Limiter la perte de données à 1 heure ou moins (RPO**)

RTO **(Recovery Time Objective) : Temps maximal toléré pour restaurer un système ou une application après une panne afin de reprendre une activité normale.*

***RPO **(Recovery Point Objective)** : Quantité maximale de données pouvant être perdue (en temps) lors d'un incident. Cela détermine la fréquence des sauvegardes.*

1.2 - Automatisation des sauvegardes

- **Objectif** :
  Réduire les erreurs humaines et garantir la régularité des sauvegardes.

- **Besoins** :
  - Mettre en place des sauvegardes automatiques
  - Programmer des sauvegardes fréquentes (quotidiennes ou horaires selon les données critiques)

1.3 - Sécurisation des sauvegardes

- **Objectif** :
  Protéger les données contre la perte ou la corruption.

- **Besoins** :
  - Stocker les sauvegardes sur un support distinct (Serveur NAS*, serveur dédié)
  - Utiliser le chiffrement AES-256 pour protéger les sauvegardes

NAS **(Network Attached Storage) : Serveur de stockage dédié, connecté au réseau, permettant de centraliser et partager des données ou sauvegardes entre plusieurs utilisateurs ou systèmes.*

1.4 - Redondance géographique

- **Objectif** :
  Assurer la résilience face aux catastrophes locales.

- **Besoins** :

    - Répliquer les sauvegardes dans des emplacements éloignés (cloud ou autre datacenter)

1.5 - Tests réguliers de restauration

- **Objectif** :
  Vérifier que les sauvegardes sont fiables et restaurables.

- **Besoins** :
    - Tester mensuellement la restauration des données
    - Garantir que les restaurations respectent les objectifs de délai (RTO)

1.6 - Conformité et traçabilité

- **Objectif** :
  Répondre aux exigences légales et assurer un suivi des opérations.

- **Besoins** :
    - Documenter les processus de sauvegarde/restauration
    - Conserver des journaux d'activité pour tracer les sauvegardes et restaurations

2. Solution sélectionnée : Solution hybride

Sauvegardes locales :
Utilisation d'un NAS pour des sauvegardes rapides et fréquentes, facilitant la restauration immédiate en cas de problème.

Sauvegardes distantes :
Réplication automatique des sauvegardes locales vers un service cloud (AWS S3, Google Cloud, Azure, etc.) pour protéger les données contre les catastrophes locales.

2.1 - Avantages

- **Disponibilité** :
  Restauration immédiate avec les sauvegardes locales.

- **Sécurité** :
  Résilience accrue grâce à la redondance géographique.

- **Automatisation** :
  Planification des sauvegardes pour éviter les erreurs humaines.

2.2 - Planification des sauvegardes

- **Sauvegardes locales** :
  Quotidiennes à 2h via un NAS.

- **Sauvegardes distantes** :
  Quotidiennes à 3h avec le service cloud AWS S3 pour réduire au minimum les risques de perte de données.

  La fréquence quotidienne répond au besoin de continuité de service, notamment dans un contexte où les utilisateurs accèdent en permanence à l'application.

2.3 - Plan de test de restauration

Fréquence des tests :
- **Tests locaux** : Mensuels.
- **Tests distants** : Trimestriels.

Procédure :
1. Restaurer un jeu de données complet sur un environnement de test.
2. Vérifier l'intégrité des données restaurées.

3. Tester les fonctionnalités critiques (authentification, catalogue, tunnel d'achat).
4. Documenter les résultats des tests.

Les tests réguliers garantissent la fiabilité et la validité des sauvegardes, minimisant ainsi les risques en cas d'incident.

2.4 - Coûts estimés

- **Infrastructure locale (NAS)** :
  - **Synology DS923+** (exemple) : ~800 €
  - **4 disques de 4 To en RAID5** (stockage) : ~500 €

- **Stockage cloud** :
  - **AWS S3 Standard :** 0,023 $/Go/mois.
  - 1 To sur un an (1000 Go x 12 x 0,023 $) : ~265,49 Euro

2.5 - Rétention des données

- **Sauvegardes locales :**
  - **Incrémentales** : Conserver les sauvegardes des 7 derniers jours.
  - **Complètes** : Conserver 30 jours de sauvegardes.
- **Sauvegardes distantes :**
  - Rétention minimale d'un mois avec possibilité d'archivage longue durée.

3. Plan de restauration des données

1. **Identifier la défaillance** :
   Repérer les signes du problème (perte de données, indisponibilité du système, corruption).

2. **Notifier les équipes** :
   Informer l'équipe chargée des sauvegardes et des restaurations pour qu'elle prenne en main la situation.

3. **Localiser la sauvegarde fonctionnelle** :
   Identifier la dernière sauvegarde saine (complète ou incrémentale).

4. **Isoler les services défaillants** :
   Mettre hors ligne les services affectés pour éviter d'aggraver la situation.

5. **Restaurer les données** :
   - Charger la sauvegarde complète depuis le stockage (local ou cloud).
   - Appliquer les sauvegardes incrémentales, si nécessaire.
   - Vérifier l'intégrité des données : Contrôler la cohérence et la complétude des données restaurées.

6. **Tester les fonctionnalités critiques** :
   Vérifier que les fonctions essentielles (authentification, catalogue, achats, etc.) fonctionnent correctement.

7. **Redémarrer les services** :
   Relancer les services une fois la restauration validée.

8. **Informer les parties prenantes** :
   Communiquer avec les utilisateurs et/ou équipes internes pour expliquer la situation et rassurer sur le rétablissement.

9. **Analyser et améliorer** :
   Documenter l'incident, ses causes et les actions entreprises. Mettre à jour le plan de sauvegarde/restauration pour prévenir des problèmes similaires à l'avenir.