Justification des Choix Technologiques

Dans le cadre de la mission de groupe visant à concevoir une plateforme de gestion et de monitoring des données bancaires pour DigitalBank, notre équipe a fait le choix d'une **architecture hybride no-code / low-code**.

L'objectif était de **concilier rapidité de mise en œuvre, sécurité, scalabilité et professionnalisme**, tout en respectant les contraintes pédagogiques du projet et les exigences d'un environnement bancaire.

Les choix technologiques ont été guidés par quatre critères principaux :

- **Sécurité et conformité** (données bancaires, RGPD, contrôle des accès)
- **Facilité d'intégration entre les composants**
- **Réduction du code custom** pour accélérer le développement
- **Lisibilité et maintenabilité** de la solution par des équipes non techniques

1. Base de Données – PostgreSQL

Choix retenu

PostgreSQL (base restaurée depuis la Partie 1)

Justification

PostgreSQL a été conservé comme socle de données pour plusieurs raisons :

- Il s'agit d'un **SGBD relationnel robuste et mature**, largement utilisé dans le secteur bancaire.
- Il offre un **haut niveau de sécurité native** (RBAC, vues, contraintes, chiffrement possible).
- La base existante issue de la Partie 1 garantit la **continuité pédagogique et fonctionnelle** du projet.
- Il est parfaitement compatible avec les outils low-code choisis (Xano, Power BI).

Alternatives envisagées

- **MySQL** : moins avancé sur les aspects de sécurité et de conformité.
- **Bases NoSQL (MongoDB)** : non adaptées à un modèle transactionnel bancaire structuré.

Critère décisif

Fiabilité, conformité et continuité avec la Partie 1

2. API Layer – Xano (Low-Code Backend)

Choix retenu

Xano

Justification

Xano a été choisi comme couche API centrale pour exposer les données PostgreSQL de manière sécurisée :

- Permet de créer des **API REST sans écrire de backend complexe**
- Gestion native de :
    - Authentification (JWT)
    - RBAC
    - Logs et monitoring des requêtes
- Séparation claire entre la base de données et le frontend, renforçant la sécurité
- Déploiement cloud rapide et scalable

Xano joue un rôle clé en tant que **pont sécurisé** entre la base de données et les outils de visualisation.

Alternatives envisagées

- **Backend custom (Flask / Spring Boot)** : plus flexible mais trop coûteux en temps et en maintenance.
- **Supabase** : moins orienté logique métier complexe et RBAC avancé.

Critère décisif

Rapidité de développement + sécurité intégrée

3. Frontend & Dashboards – Power BI

Choix retenu

Power BI

Justification

Power BI a été retenu pour la visualisation et l'analyse des données :

- Outil professionnel de **Business Intelligence**, largement utilisé en entreprise
- Connexion native à PostgreSQL et aux API
- Création rapide de :
    - Dashboards temps réel
    - Indicateurs de fraude
    - Rapports automatisés
- Gestion des rôles et de la visibilité des données selon les profils utilisateurs

Il répond parfaitement au besoin de **monitoring en temps réel et de reporting automatisé**.

Alternatives envisagées

- **Tableau** : solution équivalente mais moins accessible dans un cadre pédagogique.
- **Dashboards custom (React, Chart.js)** : trop coûteux en développement.

Critère décisif

Standard professionnel + rapidité + reporting natif

4. Automatisations – Make.com

Choix retenu

Make (ex-Integromat)

Justification

Make.com a été choisi pour orchestrer les automatisations métier :

- Détection d'événements suspects (fraude, anomalies)
- Déclenchement d'alertes (email, webhook)
- Génération automatique de rapports
- Intégration fluide avec Xano, Power BI et autres services

Make permet de **réagir automatiquement aux événements sans développement lourd**, ce qui est essentiel pour un système de sécurité réactif.

Alternatives envisagées

- **Zapier** : plus limité pour des scénarios complexes.
- **Scripts Python planifiés** : moins lisibles et moins accessibles.

Critère décisif

Puissance des scénarios + logique métier visuelle

5. Monitoring & Sécurité – Prometheus

Choix retenu

Prometheus

Justification

Prometheus est utilisé pour le monitoring technique et sécurité :

- Collecte de métriques système et applicatives

- Surveillance des performances API et base de données
- Détection des comportements anormaux
- Intégration possible avec des systèmes d'alerting

Il apporte une **vision technique complémentaire** aux dashboards fonctionnels de Power BI.

Alternatives envisagées

- **Grafana Cloud seul** : nécessite une couche de collecte.
- **Solutions propriétaires** : moins adaptées à un contexte pédagogique.

Critère décisif

Monitoring standard open-source et extensible

6. Architecture de Sécurité

Les choix technologiques s'inscrivent dans une architecture sécurisée :

- **Authentification** : JWT / OAuth via Xano
- **Contrôle d'accès** : RBAC cohérent sur toute la chaîne
- **Chiffrement** :
    - Données au repos (PostgreSQL)
    - Données en transit (HTTPS)
- **Audit & traçabilité** :
    - Logs API (Xano)
    - Logs système et métriques (Prometheus)

Cette architecture respecte les **principes du moindre privilège**, de la **défense en profondeur** et les exigences **RGPD**.

Pour conclure, les technologies retenues ont été choisies pour offrir une **solution réaliste, sécurisée et exploitable en entreprise**, tout en restant cohérente avec une approche no-code / low-code.

La plateforme proposée répond ainsi pleinement aux objectifs de DigitalBank en matière de **gestion des données, détection de fraude, sécurité et monitoring**.