

PHASE 3 — Sécurité et Conformité

Authentification, Gestion des Accès et Row Level Security

Projet DigitalBank — ESIS / CPDIA

1 Objectif de la phase

L'objectif de cette phase est de garantir la sécurité des données sensibles de la plateforme *DigitalBank* en mettant en place :

- une authentification sécurisée avec authentification multi-facteur (MFA),
- une gestion stricte des rôles utilisateurs,
- une protection des données via le mécanisme de **Row Level Security (RLS)**.

L'ensemble des contrôles d'accès est implémenté à l'aide de **Supabase** et testé via **Postman**.

—

2 Authentification et MFA

L'authentification des utilisateurs est assurée par Supabase Auth, basée sur des tokens JWT. Une authentification multi-facteur (MFA) est activée afin de renforcer la sécurité des comptes, en particulier pour les rôles sensibles comme *admin*.

Chaque utilisateur doit s'authentifier pour obtenir un token d'accès, utilisé ensuite dans les requêtes API sécurisées.

—

3 Gestion des rôles

Un système de rôles est mis en place via une table dédiée liant les utilisateurs authentifiés à leurs permissions applicatives.

3.1 Rôles définis

- **admin** : accès complet à toutes les données et opérations (lecture, modification, suppression).
- **analyst** : accès en lecture seule à l'ensemble des transactions, notamment pour la détection de fraude.
- **customer_service** : accès en lecture aux clients et transactions, avec modification limitée.
- **customer** : accès strictement limité à ses propres données (comptes et transactions).

—

4 Row Level Security (RLS)

Le mécanisme de **Row Level Security** est activé sur toutes les tables sensibles :

- customers
- accounts
- transactions
- audit_logs

Les politiques RLS permettent de filtrer les données retournées ou modifiées en fonction :

- du rôle de l'utilisateur,
- de son identifiant unique (`auth.uid()`),
- de la propriété des données (par exemple : un client ne peut accéder qu'à ses propres comptes).

Ce mécanisme garantit qu'aucune donnée non autorisée n'est exposée, même en cas de requête directe via l'API.

—

5 Tests des permissions

Les permissions ont été testées via l'outil Postman pour chaque rôle :

5.1 Admin

- Consultation de toutes les tables (GET) : autorisée
- Modification et suppression des données (PATCH / DELETE) : autorisées

5.2 Analyst

- Consultation globale des transactions : autorisée
- Création, modification et suppression : refusées

5.3 Customer Service

- Lecture des clients et transactions : autorisée
- Suppression des données sensibles : refusée

5.4 Customer

- Consultation de ses propres comptes et transactions : autorisée
- Accès aux données des autres clients : refusé
- Création, modification ou suppression : refusées

Les résultats des tests sont illustrés par des captures d'écran jointes au livrable.

—

6 Conclusion

La mise en place conjointe de l'authentification sécurisée, de la gestion des rôles et du Row Level Security permet de garantir un haut niveau de sécurité et de conformité. Les contrôles d'accès sont stricts, traçables et alignés avec les exigences du cahier des charges.