

ARCHITECTURE & SÉCURITÉ

Conception d'une plateforme SaaS multi-tenant sécurisée pour BEYIMA

1. Contexte et objectifs

BEYIMA est une plateforme SaaS destinée à plusieurs entreprises africaines opérant dans des domaines critiques tels que le paiement, l'ERP, les ressources humaines et la FinTech. L'objectif est de concevoir une architecture multi-tenant sécurisée, scalable et résiliente.

2. Gestion des tenants (Multi-tenancy)

- * Multi-tenant logique avec une base partagée.
- * Isolation des données via le champ `tenant_id`.
- * Middleware backend pour filtrer automatiquement par `tenant_id`.

3. Authentification & gestion des identités

- * JWT (access + refresh tokens), mots de passe hachés avec bcrypt.
- * Rotation des tokens et MFA pour comptes sensibles.

4. Rôles et permissions (RBAC)

- * Rôles par tenant : Admin, Manager, User, Finance, RH.
- * Permissions explicites vérifiées via guards/middleware.

5. Sécurité API

- * HTTPS obligatoire, CORS strict, rate limiting.
- * Validation stricte des payloads et journalisation des actions sensibles.

6. Scalabilité & performance

- * Backend stateless, frontend SPA.
- * Déploiement conteneurisé (Docker), scaling horizontal.
- * Cache Redis pour sessions et données fréquentes.

7. Intégration des APIs tierces (Mobile Money)

- * Module dédié aux paiements, abstraction des fournisseurs.
- * Webhooks sécurisés et gestion des secrets.

8. CI/CD et déploiement

- * GitHub Actions/GitLab CI : tests, sécurité, build Docker, déploiement.
- * Environnements séparés, rollback automatique, monitoring.

9. Conclusion

La plateforme BEYIMA garantit isolation des données, sécurité, scalabilité et intégration avec les systèmes africains de paiement, pour une solution SaaS fiable et performante.