# Thiết kế microservice KYC cho EchoFi

## 1. Mục tiêu

• Đảm bảo tuân thủ quy định AML/KYC quốc tế (FATF, EU 5AMLD, NHNN VN).  
• Xác thực danh tính người dùng trước khi cho phép rút/mint ECHO.  
• Tích hợp mượt mà trên Web, Mobile, Telegram Mini-App.  
• Bảo mật dữ liệu cá nhân: mã hóa, audit trail, “right to be forgotten”.

## 2. Yêu cầu chức năng

• Thu thập thông tin cá nhân (họ tên, ngày sinh, địa chỉ, email, điện thoại).

• Cho phép tải lên giấy tờ (CMND/CCCD, Hộ chiếu, GPLX; trước/sau).

• Selfie/video liveness so khớp với ảnh giấy tờ.

• OCR tự động và đối chiếu khuôn mặt.

• Phân tầng KYC: Tier 0 (view), Tier 1 (rút giới hạn), Tier 2 (full).

• Dashboard admin để duyệt/chặn và ghi chú manual review.

• Audit logs cho mọi hành động và trạng thái.

• Thông báo trạng thái qua email/Telegram.

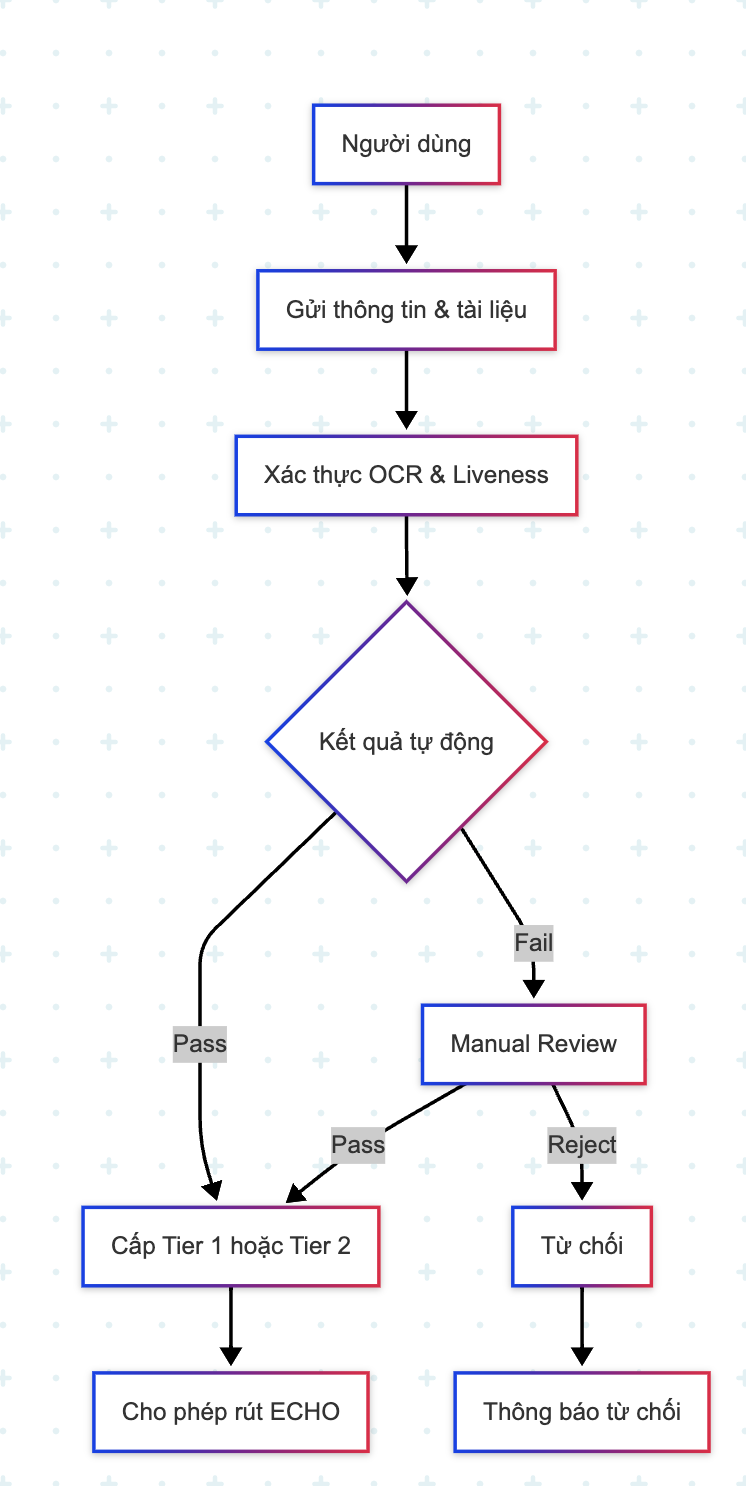
• API Smart-Contract: chỉ cho phép rút khi KYC đạt.

## 3. Yêu cầu phi chức năng

• AES-256 mã hóa dữ liệu; TLS1.3 in-transit.  
• GDPR/PDPA: lưu giữ tối đa 5 năm; hỗ trợ xóa dữ liệu.  
• Hiệu năng: ≥ 1000 yêu cầu/ngày; P95 OCR < 2s.  
• SLA ≥ 99.9%; kiến trúc microservices, pluggable provider.

## 4. Lược đồ quy trình KYC

```mermaid  
flowchart TD  
 A[Người dùng] --> B[Gửi thông tin & tài liệu]  
 B --> C[Xác thực OCR & Liveness]  
 C --> D{Kết quả tự động}  
 D -->|Pass| E[Cấp Tier 1 hoặc Tier 2]  
 D -->|Fail| F[Manual Review]  
 F -->|Pass| E  
 F -->|Reject| G[Từ chối]  
 E --> H[Cho phép rút ECHO]  
 G --> I[Thông báo từ chối]  
```



## 5. Kiến trúc tổng quan

Web/Mobile/Telegram UI → API Gateway → Microservice KYC → Provider (Onfido/Jumio/self-host CV model analyze like tesseract (more info in [ref](https://salv.com/blog/best-kyc-software-and-tools/#:~:text=tr%C6%B0%E1%BB%9Fng%20nhanh%20h%C6%A1n.-,Onfido,hi%E1%BB%87u%20ph%C3%A1t%20hi%E1%BB%87n%20gian%20l%E1%BA%ADn.))) → Database (đã mã hóa) → (mint/lock/ect…). Dashboard Admin và Audit Store kết nối vào Backend.

## 6. Dependencies

1. **Onfido Smart Capture SDK** – Cung cấp giao diện chụp giấy tờ, kiểm tra độ nhòe, liveness detection cho web/mobile
2. **Sumsub Identity Verification API** – Tự động xác thực giấy tờ và non-doc verification qua REST API
3. **LSEG World-Check One** – Dịch vụ PEP/sanctions screening với dữ liệu proprietary
4. **Amazon Textract** – OCR ML để trích xuất text, bảng, form từ hình ảnh/PDF
5. **Google Cloud Vision API** (DOCUMENT\_TEXT\_DETECTION) – OCR tài liệu dày ký tự, handwriting
6. **Azure Computer Vision OCR** – Dịch vụ OCR doanh nghiệp với bảo mật cao
7. **Amazon Rekognition Identity Verification** – Biometric face-match, liveness check, spoof detection
8. **OFAC Sanctions List Service** – Cập nhật danh sách SDN/Consolidated để screening
9. **ComplyAdvantage API** – AML real-time checks (sanctions, PEP, adverse media)
10. **PostgreSQL** – Cơ sở dữ liệu chính, hỗ trợ pgcrypto để mã hóa column‐level
11. **AWS S3 + KMS** – Lưu trữ tài liệu với SSE-KMS, quản lý khóa bằng KMS
12. **Docker & Kubernetes** – Containerization và orchestration microservices
13. **RabbitMQ** – Message broker để xử lý bất đồng bộ giữa các service

**Vai trò**

* **Xác thực danh tính (1–3)**: Onfido và Sumsub hỗ trợ capture, OCR, liveness, còn World-Check One cung cấp data PEP/sanctions giúp tuân thủ AML  .
* **Xử lý tài liệu (4–6)**: Textract, Cloud Vision, Azure OCR giúp tự động hóa trích xuất thông tin từ giấy tờ, giảm sai sót con người  .
* **Sinh trắc học (7)**: Rekognition đảm bảo face-match và liveness quality cao, API dễ tích hợp  .
* **Lọc rủi ro (8–9)**: OFAC SLS & ComplyAdvantage liên tục cập nhật watchlists, tránh đói tượng bị blacklist hoặc KYC không đủ điều kiện thực hiện.
* **Hạ tầng lưu trữ (10–11)**: PostgreSQL + pgcrypto và S3 SSE-KMS đảm bảo dữ liệu cá nhân mã hóa at-rest, key management an toàn .
* **Triển khai & Messaging (12–13)**: Docker/K8s giúp scale microservices, RabbitMQ xử queue high-throughput, đảm bảo tính sẵn sàng cao và decoupling .