

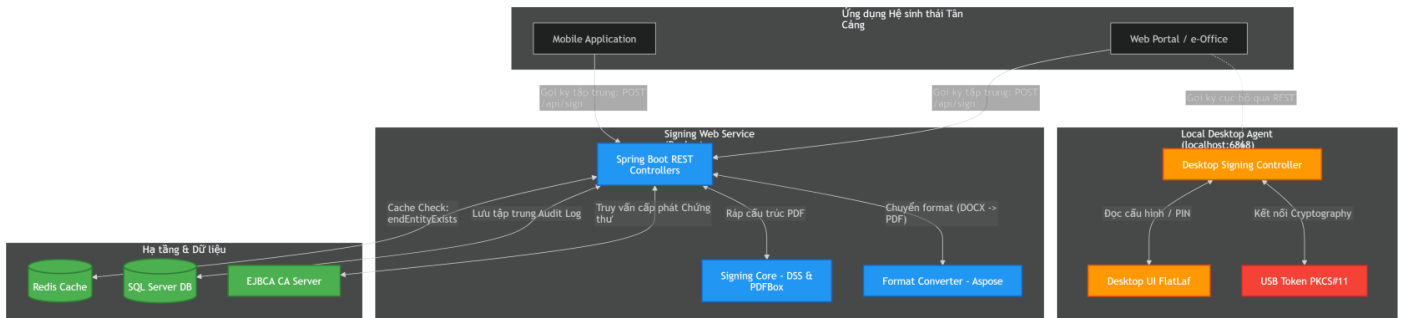
# Chương 3: Kiến trúc Hệ thống & Cổng giao tiếp API

Chương này trình bày cái nhìn tổng quát về mô hình triển khai của hệ thống Signing Service Tân Cảng, sự tương tác giữa các vi dịch vụ, cũng như chi tiết đặc tả các cổng giao tiếp (API Interfaces) để các bên thứ 3 hoặc các nền tảng e-Office tích hợp.

- [3.1. Sơ đồ Kiến trúc Tổng thể \(System Architecture\)](#)
- [3.2. Danh sách Web API Chính \(Server-Side\)](#)
- [3.3. Danh sách Desktop API \(Cục bộ localhost:6868\)](#)

# 3.1. Sơ đồ Kiến trúc Tổng thể (System Architecture)

Giải pháp được xây dựng theo mô hình **Client-Server phân tán (Distributed)** kết hợp bộ đệm (Cache) và kiến trúc Agent cục bộ dành cho chữ ký cứng.



## Thành phần chính:

- Signing Web Service (Server):** Điểm vào chính của các yêu cầu ký tập trung. Bao gồm bộ Converter (Aspose) và Signing Core (DSS/PDFBox) xử lý dữ liệu chuẩn PAdES.
- Local Desktop Agent (Client):** Ứng dụng trung gian giúp Web Browser truy xuất trực tiếp chứng thư số từ USB vật lý (không bị trình duyệt chặn giao thức bảo mật) dựa vào endpoint REST API cục bộ.
- Hạ tầng hỗ trợ (Redis/MSSQL):** Redis giúp cache `EJBCAService` tránh tải nặng cho CA nội bộ với mỗi lượt request. SQL Server (MSSQL) lưu log và phân quyền truy cập.

# 3.2. Danh sách Web API Chính (Server-Side)

Đây là các endpoint chủ lực trên máy chủ (nằm trong SigningController), sử dụng JSON làm phương tiện trao đổi (`application/json` hoặc `multipart/form-data`). Hệ thống yêu cầu Header `Token-Signing` (phiên ký hợp lệ) cho hầu hết các API nghiệp vụ.

## 1. Nhóm API Xác thực OTP & Cấp quyền

- **POST /api/sign/request-otp**: Yêu cầu tạo mã OTP từ hệ thống. Dùng cho luồng bảo mật bước 2.
- **POST /api/sign/verify-otp**: Xác thực OTP để hệ thống cấp/kiểm tra phiên ký hợp lệ.

## 2. Nhóm API Ký số & Xử lý Tài liệu

- **POST /api/sign/document**:
  - API chính để ký dữ liệu tập trung (Dùng chứng thư máy chủ EJBCA).
  - **Input**: Hỗ trợ Upload File (`@ModelAttribute WebSignRequestDTO`), tự động nhận diện định dạng (DOCX, XLSX, PDF) để convert qua PDF.
- **POST /api/sign/document-with-image** & **POST /api/sign/documents-with-image**:
  - Hỗ trợ ký số và chèn ảnh (Visual Signature). Yêu cầu truyền mảng `imageMetadata` chứa thông tin tọa độ.
- **POST /api/sign/document-initial-signature**:
  - Chuyên dùng cho nghiệp vụ Ký nháy, chèn hình ảnh/con dấu chữ ký ở các tọa độ linh hoạt.

## 3. Nhóm API Quản trị & Audit Log

- **GET /api/admin/audit-logs/range** (Controller: `AuditLogAdminController`): Lấy danh sách vết giao dịch ký.
- **GET /api/agnostic/test-connection** (Controller: `EmailDiagnosticController`): Gửi cảnh báo SMS/Email kiểm tra tình trạng kết

# 3.3. Danh sách Desktop API (Cục bộ localhost:6868)

Để tiện cho Web frontend gửi lệnh ký vào máy trạm, ứng dụng Desktop mở sẵn cổng RESTful trực tiếp trên máy người dùng (qua DesktopSigningController). Các endpoint này giao tiếp trực tiếp với USB Token.

- **POST /api/desktop/sign** : Endpoint ký file PDF cơ bản.
- **POST /api/desktop/document** : Endpoint ký hỗ trợ convert file (Word, Excel) trước khi ký.
- **POST /api/desktop/document-with-image** : Endpoint ký và chèn hình ảnh con dấu (Tương đương chức năng trên Server nhưng ký bằng Token Local). Hỗ trợ xác định vị trí chèn ảnh chèn lấp (OVERLAY), trái (LEFT), phải (RIGHT) v.v.