**🧭 Tổng quan dự án: RemoteCLI\_App**

* **Controller (Máy A):** Ứng dụng người dùng, cho phép kết nối đến máy Agent và gửi lệnh command.
* **Agent (Máy B):** Ứng dụng nền (service), lắng nghe kết nối từ Controller, nhận lệnh, chạy trên cmd/powershell rồi trả kết quả.

RemoteCLI\_App/

│

├── controller/ ← Máy A: app điều khiển

│ ├── main\_controller.py ← Điểm khởi chạy app (GUI / CLI)

│ ├── ui/ ← Giao diện người dùng

│ │ ├── main\_window.py ← Giao diện chính: danh sách agent, command box

│ │ ├── pairing\_window.py ← Cửa sổ nhập token / quét QR

│ │ └── logs\_view.py ← Hiển thị log & lịch sử lệnh

│ │

│ ├── network/ ← Quản lý kết nối mạng

│ │ ├── discovery\_client.py ← Lắng nghe UDP broadcast từ Agent

│ │ ├── controller\_client.py ← Gửi command, nhận result (TLS socket)

│ │ └── tls\_context.py ← Tạo SSLContext & xác thực fingerprint

│ │

│ ├── pairing/ ← Ghép cặp với Agent

│ │ ├── pairing\_manager.py ← Gửi yêu cầu pairing, lưu peer info

│ │ ├── qr\_reader.py ← (Tùy chọn) đọc mã QR từ webcam/token

│ │ └── trusted\_peers.json ← Lưu các Agent đã được ghép nối

│ │

│ ├── core/ ← Thành phần lõi

│ │ ├── command\_executor.py ← Gửi command qua socket, nhận kết quả

│ │ ├── session\_manager.py ← Quản lý các kết nối tới nhiều Agent

│ │ ├── log\_manager.py ← Lưu và hiển thị lịch sử thực thi

│ │ └── config.py ← Cấu hình chung (port, cert path, token)

│ │

│ └── assets/ ← Icon, logo, cert mặc định

│

│

└── agent/ ← Máy B: app bị điều khiển

├── main\_agent.py ← Điểm khởi chạy chính (Service hoặc CLI)

├── network/

│ ├── agent\_server.py ← Lắng nghe TLS socket, xử lý request

│ ├── discovery\_beacon.py ← Gửi UDP broadcast thông báo hiện diện

│ └── tls\_context.py ← Tạo SSLContext server (self-signed cert)

│

├── pairing/

│ ├── pairing\_manager.py ← Xác thực pairing request từ Controller

│ ├── token\_generator.py ← Sinh token/QR code lần đầu

│ ├── paired\_clients.json ← Lưu Controller đã cho phép

│ └── pairing\_ui.py ← Popup chấp nhận pairing (nếu có GUI)

│

├── executor/

│ ├── command\_executor.py ← Thực thi command an toàn (PowerShell/cmd)

│ ├── sandbox.py ← (Tùy chọn) Giới hạn quyền & timeout

│ └── result\_formatter.py ← Chuẩn hóa output stdout/stderr/json

│

├── core/

│ ├── config.py ← Port, cert, token path

│ ├── log\_manager.py ← Ghi log truy cập & hành động

│ ├── service\_manager.py ← Tích hợp Windows Service

│ └── updater.py ← (Tùy chọn) Tự cập nhật agent

│

└── assets/

├── agent\_cert.pem

├── agent\_key.pem

└── token\_qr.png

**💻 PHÍA CONTROLLER (Máy A)**

**🟢 main\_controller.py**

* File **chính để khởi chạy app điều khiển**.
* Khởi tạo giao diện (ui/main\_window.py) + load cấu hình (core/config.py).
* Chạy vòng lặp chính (main loop GUI hoặc CLI).

**📁 ui/ – Giao diện người dùng**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **main\_window.py** | Màn hình chính: danh sách agent khả dụng, khung nhập command, hiển thị output. |
| **pairing\_window.py** | Cửa sổ để nhập token/QR khi ghép nối agent lần đầu. |
| **logs\_view.py** | Giao diện xem lại lịch sử lệnh đã gửi và kết quả nhận được. |

**📁 network/ – Kết nối mạng**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **discovery\_client.py** | Dò tìm các Agent đang chạy trong mạng LAN (qua UDP broadcast). |
| **controller\_client.py** | Quản lý socket/TLS kết nối đến Agent (gửi command, nhận kết quả). |
| **tls\_context.py** | Tạo chứng chỉ SSL/TLS và xác thực fingerprint khi bắt tay kết nối. |

**📁 pairing/ – Ghép cặp an toàn**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **pairing\_manager.py** | Gửi yêu cầu ghép cặp đến Agent, xác thực token, lưu thông tin Agent tin cậy. |
| **qr\_reader.py** | Đọc mã QR (từ camera hoặc ảnh) để tự động lấy token ghép nối. |
| **trusted\_peers.json** | File dữ liệu lưu danh sách các Agent đã được ghép cặp thành công (được phép kết nối). |

**📁 core/ – Lõi xử lý chính**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **command\_executor.py** | Xử lý việc gửi lệnh đến Agent và nhận kết quả trả về. |
| **session\_manager.py** | Quản lý nhiều kết nối đồng thời tới nhiều Agent. |
| **log\_manager.py** | Lưu log hoạt động và kết quả thực thi command. |
| **config.py** | Chứa cấu hình toàn cục: port, timeout, cert path, … |

**📁 assets/**

* Lưu **icon, logo, template cấu hình, chứng chỉ tạm** (nếu cần cho TLS).

**🖥️ PHÍA AGENT (Máy B)**

**🔵 main\_agent.py**

* File **chạy chính của Agent**, có thể đăng ký làm **Windows Service**.
* Khởi tạo cấu hình (core/config.py), sinh token lần đầu, chạy server lắng nghe (network/agent\_server.py).
* Tự động phát “beacon” UDP để Controller phát hiện.

**📁 network/ – Giao tiếp mạng**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **agent\_server.py** | Mở cổng TCP/TLS, nhận kết nối từ Controller, xử lý yêu cầu command. |
| **discovery\_beacon.py** | Phát tín hiệu UDP định kỳ để thông báo "Agent đang online". |
| **tls\_context.py** | Tạo chứng chỉ và SSLContext để thiết lập kết nối bảo mật. |

**📁 pairing/ – Ghép nối và xác thực**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **pairing\_manager.py** | Kiểm tra token khi Controller gửi yêu cầu ghép cặp; lưu Controller đã được chấp nhận. |
| **token\_generator.py** | Sinh mã token hoặc QR để Controller nhập khi ghép nối. |
| **paired\_clients.json** | Lưu danh sách Controller đã được cho phép điều khiển. |
| **pairing\_ui.py** | Giao diện popup (nếu có GUI) hiển thị yêu cầu ghép nối và nút “Chấp nhận / Từ chối”. |

**📁 executor/ – Xử lý command**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **command\_executor.py** | Nhận command từ Controller, chạy bằng subprocess, trả lại stdout/stderr. |
| **sandbox.py** | (Tuỳ chọn) Giới hạn quyền, thời gian chạy, thư mục an toàn. |
| **result\_formatter.py** | Định dạng kết quả trả về (text hoặc JSON), gồm mã lỗi, output, thời gian chạy. |

**📁 core/ – Lõi của Agent**

| **File** | **Nhiệm vụ** |
| --- | --- |
| **config.py** | Thiết lập cổng, token path, chứng chỉ TLS, timeout, … |
| **log\_manager.py** | Lưu log về các kết nối, lệnh đã chạy, lỗi. |
| **service\_manager.py** | Quản lý Agent chạy như Windows Service (cài, gỡ, start/stop). |
| **updater.py** | (Tuỳ chọn) Cho phép Agent tự cập nhật phiên bản mới từ Controller. |

**📁 assets/**

| **File** | **Mô tả** |
| --- | --- |
| **agent\_cert.pem** | Chứng chỉ công khai của Agent (TLS). |
| **agent\_key.pem** | Khoá riêng (private key) dùng cho TLS. |
| **token\_qr.png** | Mã QR chứa token pairing (dễ quét từ máy Controller). |

# Tổng kết mối quan hệ

| **Thành phần** | **Controller** | **Agent** |
| --- | --- | --- |
| **Khởi chạy** | main\_controller.py | main\_agent.py |
| **Ghép cặp** | pairing\_manager.py, qr\_reader.py | pairing\_manager.py, token\_generator.py |
| **Mạng / TLS** | controller\_client.py | agent\_server.py |
| **Thực thi lệnh** | command\_executor.py | executor/command\_executor.py |
| **Quản lý phiên** | session\_manager.py | paired\_clients.json |
| **Giao diện** | ui/ | pairing\_ui.py |
| **Ghi log** | log\_manager.py | log\_manager.py |