Sec-WebSocket-Key

1. Các khái niệm cơ bản.

- Sec-WebSocket-Key : sử dụng trong quá trình bắt tay mở websocket cho phép máy khách (tác nhân người dùng) xác nhận rằng nó “thực sự muốn” yêu cầu nâng cấp máy khác http thành websocket.

2. Cú pháp hợp lệ.

Sec-WebSocket-Key: <key>

3. Hoạt động.

- Client gửi yêu cầu Upgrade (từ HTTP → WebSocket)

- xử lí Server :

- Ghép key với 1 chuỗi cố định
- Chuỗi cần hash
- Hash bằng SHA-1 → mã hoá base64
- Trả về response

4. mục đích.

- chống lại các request giả mạo (giả mạo websocket handshake)

- xác thực hánhake websocket

- tuân thủ chuẩn RFC 6455