**1. JWT (JSON Web Token)**

* **Cách hoạt động**: Sau khi người dùng đăng nhập thành công, server trả về một token (JWT) chứa thông tin người dùng. Token này sẽ được gửi trong Authorization: Bearer <token> trong các request sau.
* **Ưu điểm**:
  + Phổ biến, chuẩn công nghiệp.
  + Stateless – không cần lưu session phía server.
  + Dễ tích hợp với frontend SPA (React, Angular...).
* **Nhược điểm**:
  + Khó thu hồi token sớm (nếu không dùng blacklist hoặc refresh token).
  + Không lưu trạng thái nên khó kiểm soát phiên.

✅ **Phù hợp**: API độc lập, mobile app, SPA frontend.

**2. Cookie-based Authentication**

* **Cách hoạt động**: Sau khi đăng nhập, server tạo một session lưu trữ trạng thái người dùng và gửi cookie session về cho client. Mỗi request sau gửi kèm cookie.
* **Ưu điểm**:
  + Tích hợp dễ với trình duyệt.
  + Hỗ trợ tốt CSRF protection.
* **Nhược điểm**:
  + Không phù hợp cho API thuần túy hoặc mobile app.
  + Khó mở rộng sang dịch vụ khác nếu không chia sẻ session.

✅ **Phù hợp**: Ứng dụng web truyền thống dùng trình duyệt.

**3. OAuth2 / OpenID Connect**

* **Cách hoạt động**: Sử dụng bên thứ ba (Google, Facebook, Azure AD...) để xác thực. Thường dùng flow Authorization Code hoặc Client Credentials.
* **Ưu điểm**:
  + Bảo mật cao, chuẩn công nghiệp.
  + Có thể dùng cho SSO.
  + Dễ mở rộng, tích hợp dịch vụ bên ngoài.
* **Nhược điểm**:
  + Cấu hình phức tạp hơn.
  + Đòi hỏi nhiều kiến thức về protocol.

✅ **Phù hợp**: Hệ thống lớn, cần login qua bên thứ 3, SSO, doanh nghiệp.

**4. API Key**

* **Cách hoạt động**: Mỗi client được cấp một key tĩnh dùng để truy cập API.
* **Ưu điểm**:
  + Dễ triển khai.
  + Hữu ích cho máy-máy, hệ thống backend.
* **Nhược điểm**:
  + Không bảo mật bằng JWT/OAuth2.
  + Không phù hợp để bảo vệ người dùng.

✅ **Phù hợp**: Hệ thống nội bộ, service-to-service.

**5. Basic Authentication (ít dùng)**

* **Cách hoạt động**: Gửi username:password trong mỗi request (dùng base64).
* **Ưu điểm**: Đơn giản, nhanh chóng cho testing.
* **Nhược điểm**: Không bảo mật trừ khi dùng HTTPS, không nên dùng production.

✅ **Phù hợp**: Testing, prototyping.