Security

Motivation for Security

application
network
system
data
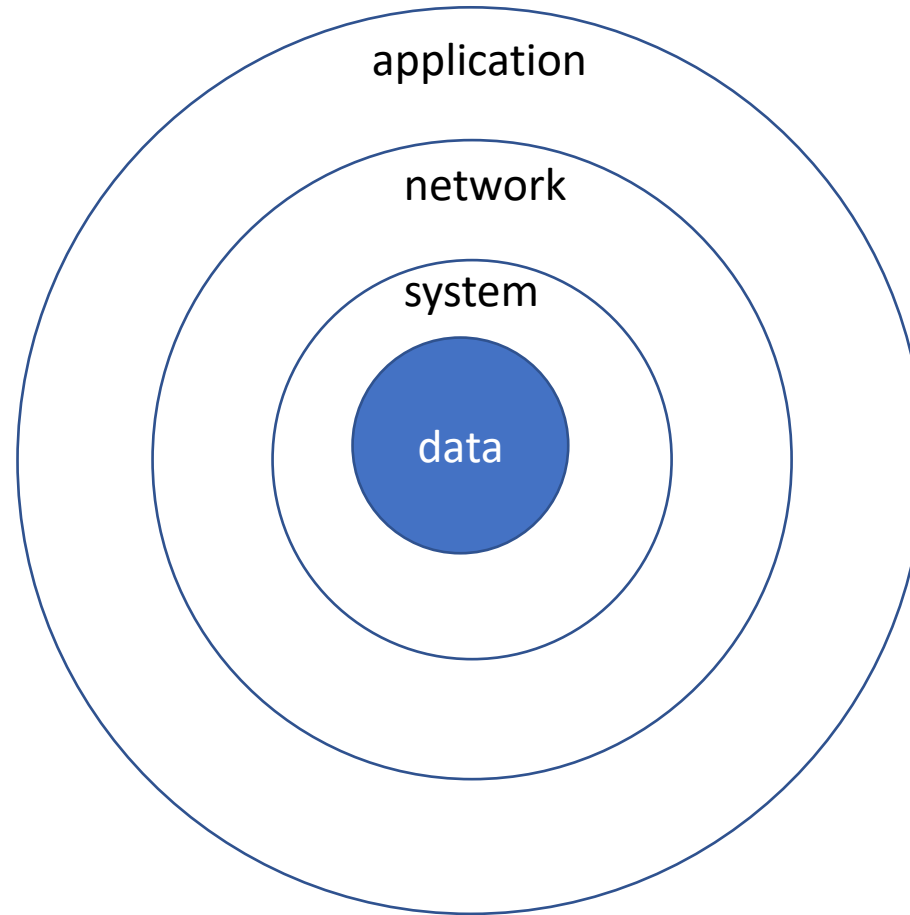
Security

→ Application Security

   → Authentication – Http 401 - Unauthorized

   → Authorization – Http 403 – Access denied

Authentication

→ Form Login

→ HTTP Basic

→ LDAP

→ Biometrics/Retina

→ OTP/TOTP

→ Chip and Pin

→ MFA

→ NFC

→ Face-recognition

→ Kerberos

→ Certificates

→ RSA soft token

→ Oauth 2.0

Authorization

→ Path based
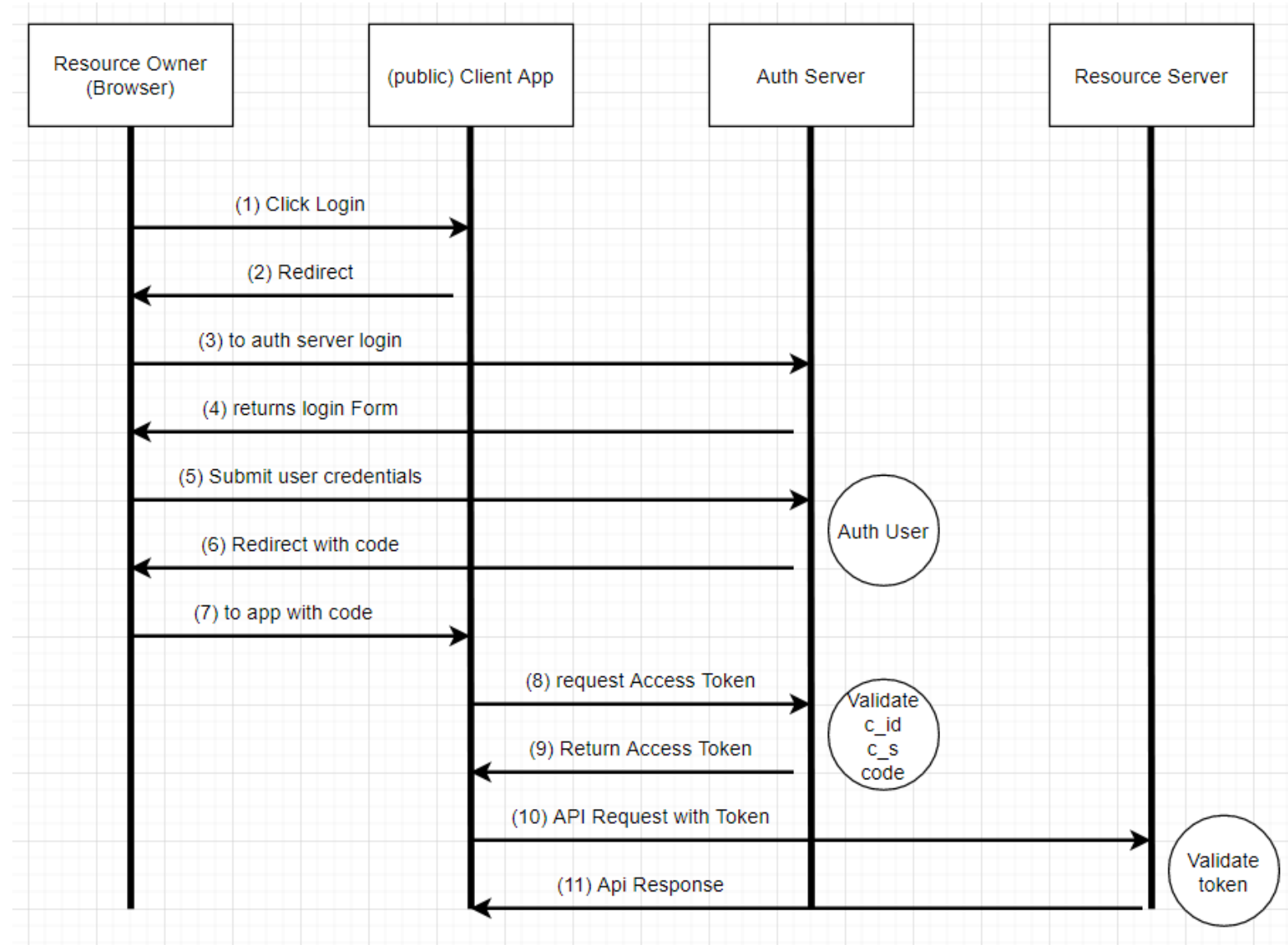
→ Method level Authorization

OAuth 2.0
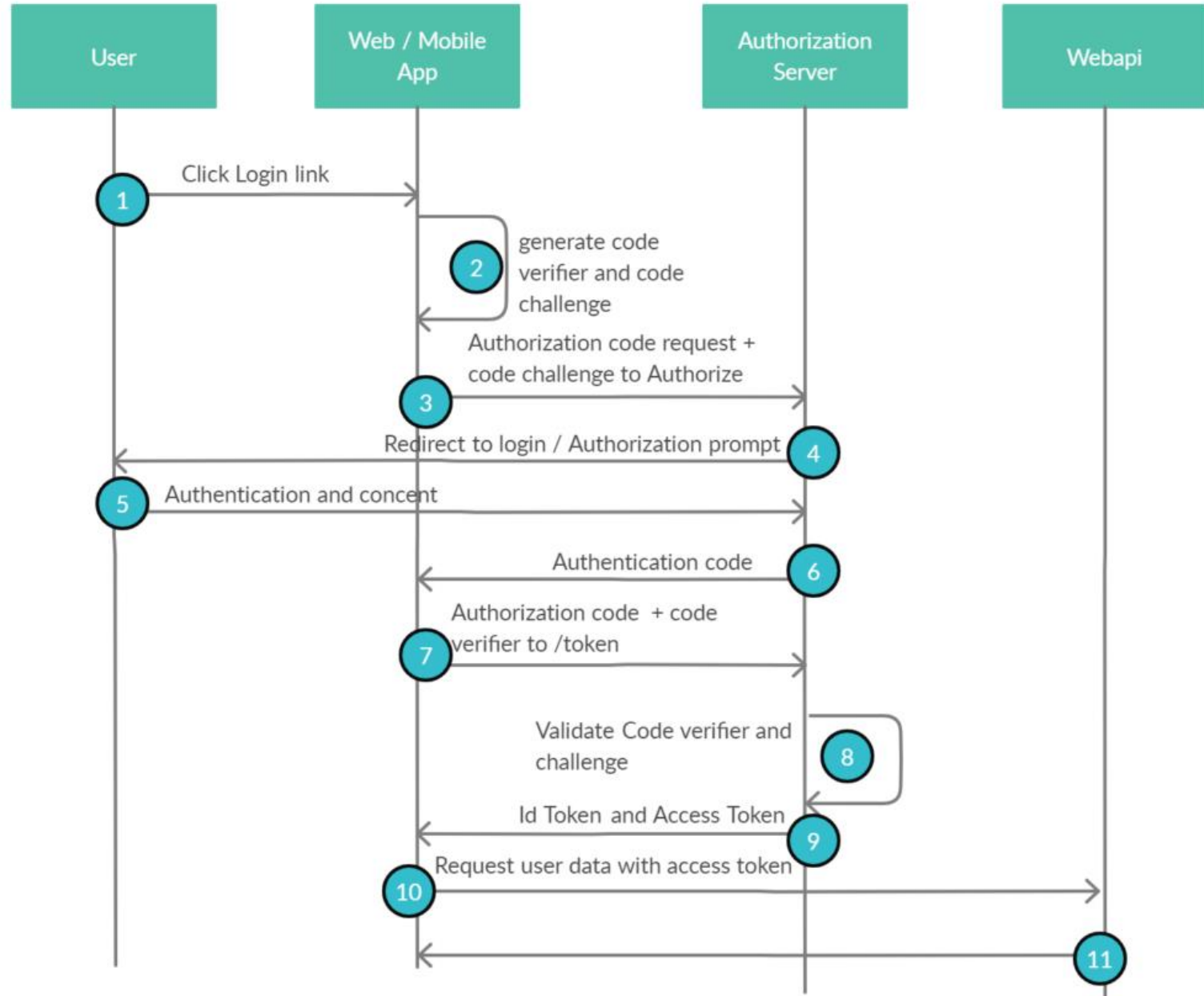
→ Delegation based

→ Used Token for Authn and Authz

Oauth 2.0

→ Resource Owner

→ Resource Server
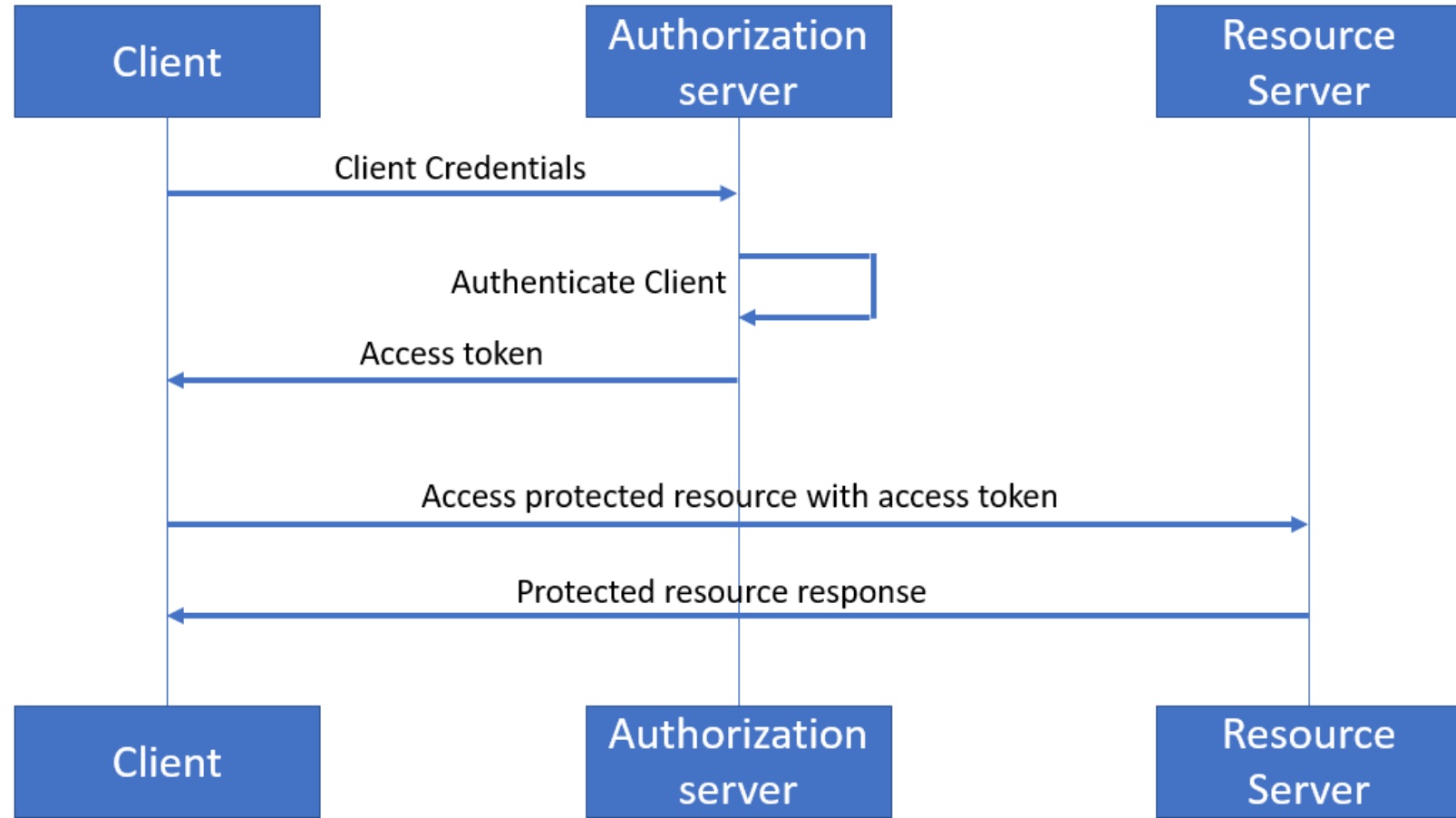
→ Authorization Server

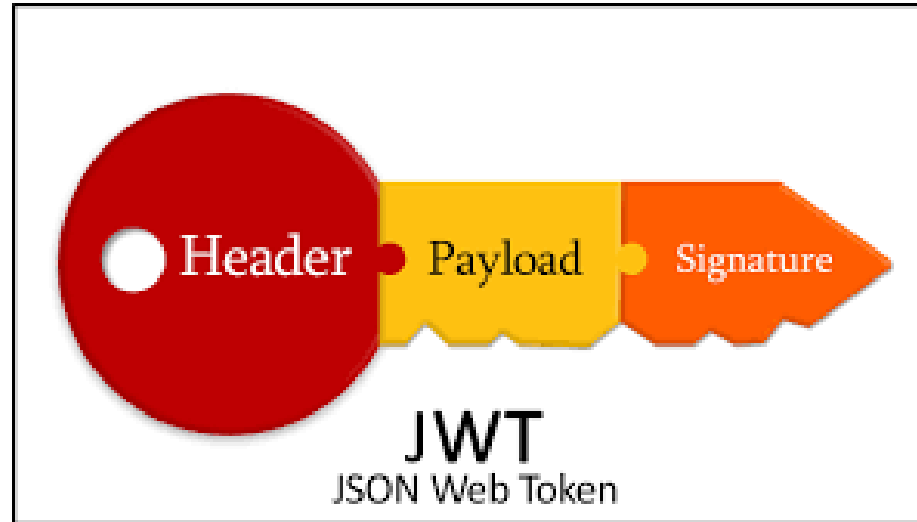→ Client application

OAuth2.0
Auth_code

OAuth2.0 PKCE

User — **Web / Mobile App** — **Authorization Server** — **Webapi**

1. Click Login link (User → Web / Mobile App)
2. generate code verifier and code challenge (Web / Mobile App self)
3. Authorization code request + code challenge to Authorize (Web / Mobile App → Authorization Server)
4. Redirect to login / Authorization prompt (Authorization Server → User)
5. Authentication and concent (User → Authorization Server)
6. Authentication code (Authorization Server → Web / Mobile App)
7. Authorization code + code verifier to /token (Web / Mobile App → Authorization Server)
8. Validate Code verifier and challenge (Authorization Server self)
9. Id Token and Access Token (Authorization Server → Web / Mobile App)
10. Request user data with access token (Web / Mobile App → Webapi)
11. (Webapi → Web / Mobile App)

OAuth2.0
Client credentials

JSON Web Token

JWKS endpoint

→ URI is public endpoint

→ JWK is a JSON object that represents a cryptographic key

→ JWKS has array of JWK