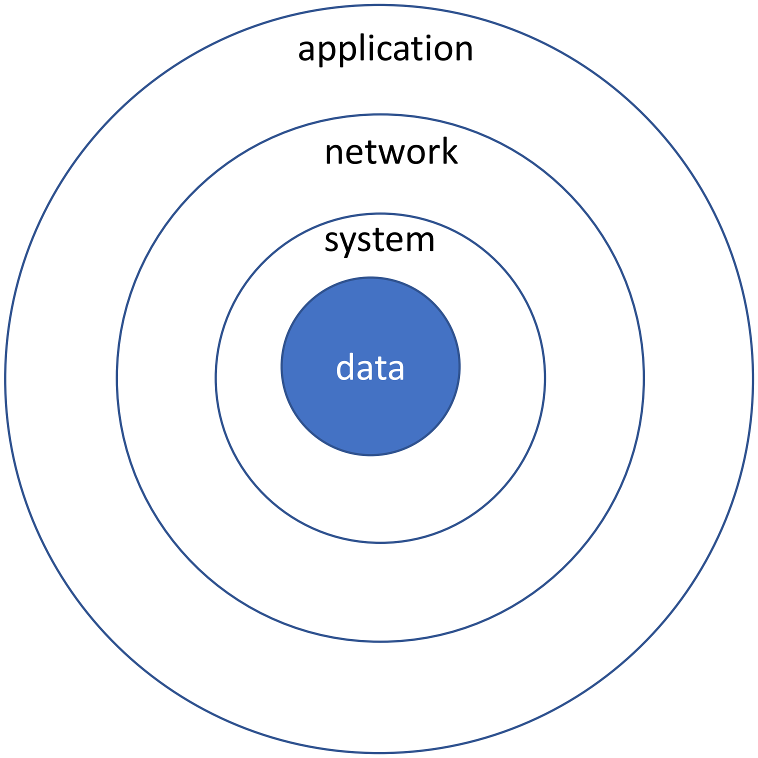
Security

Motivation for Security



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

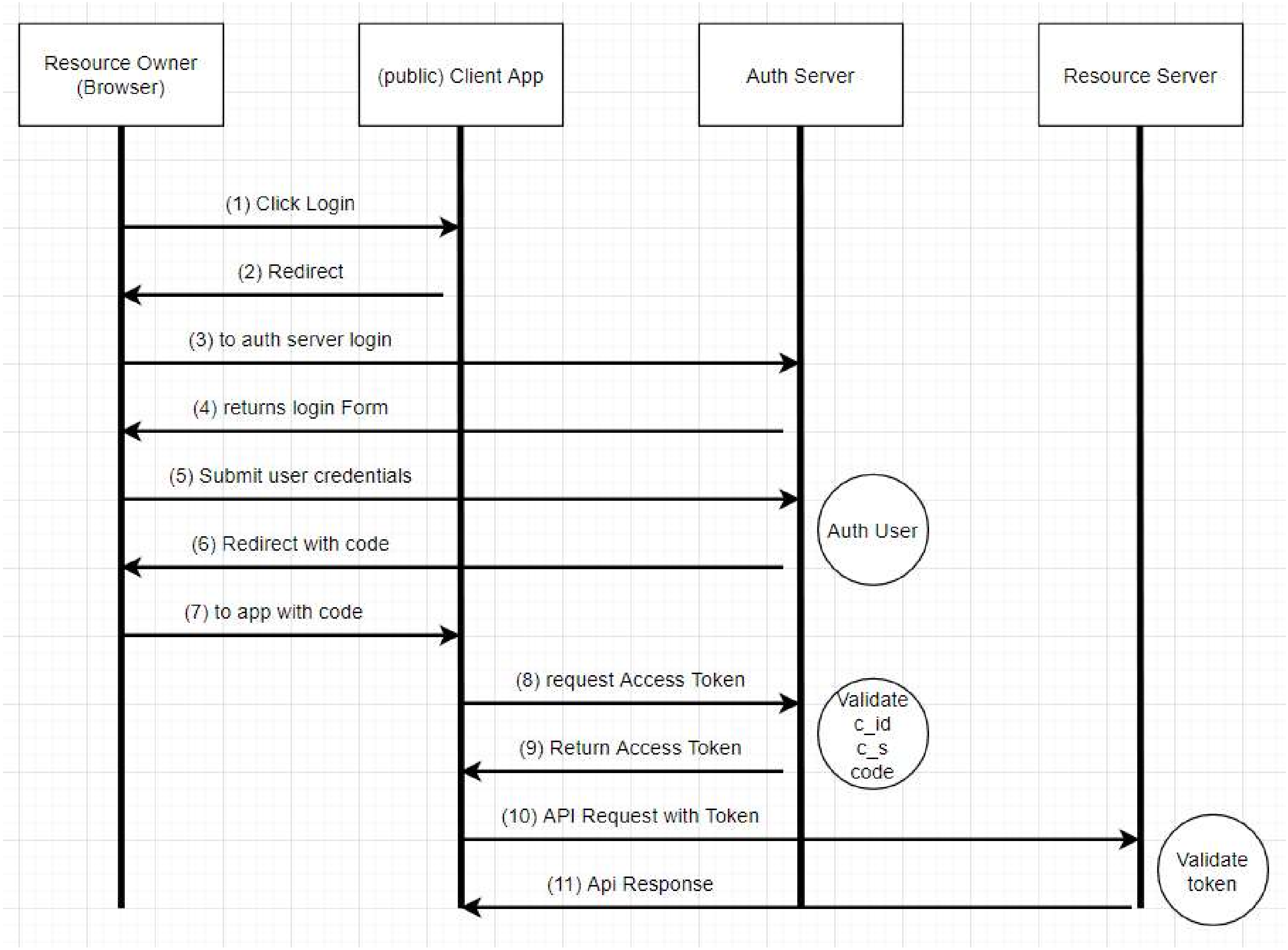
OAuth 2.0

- → Delegation based
- → Used Token for Authn and Authz

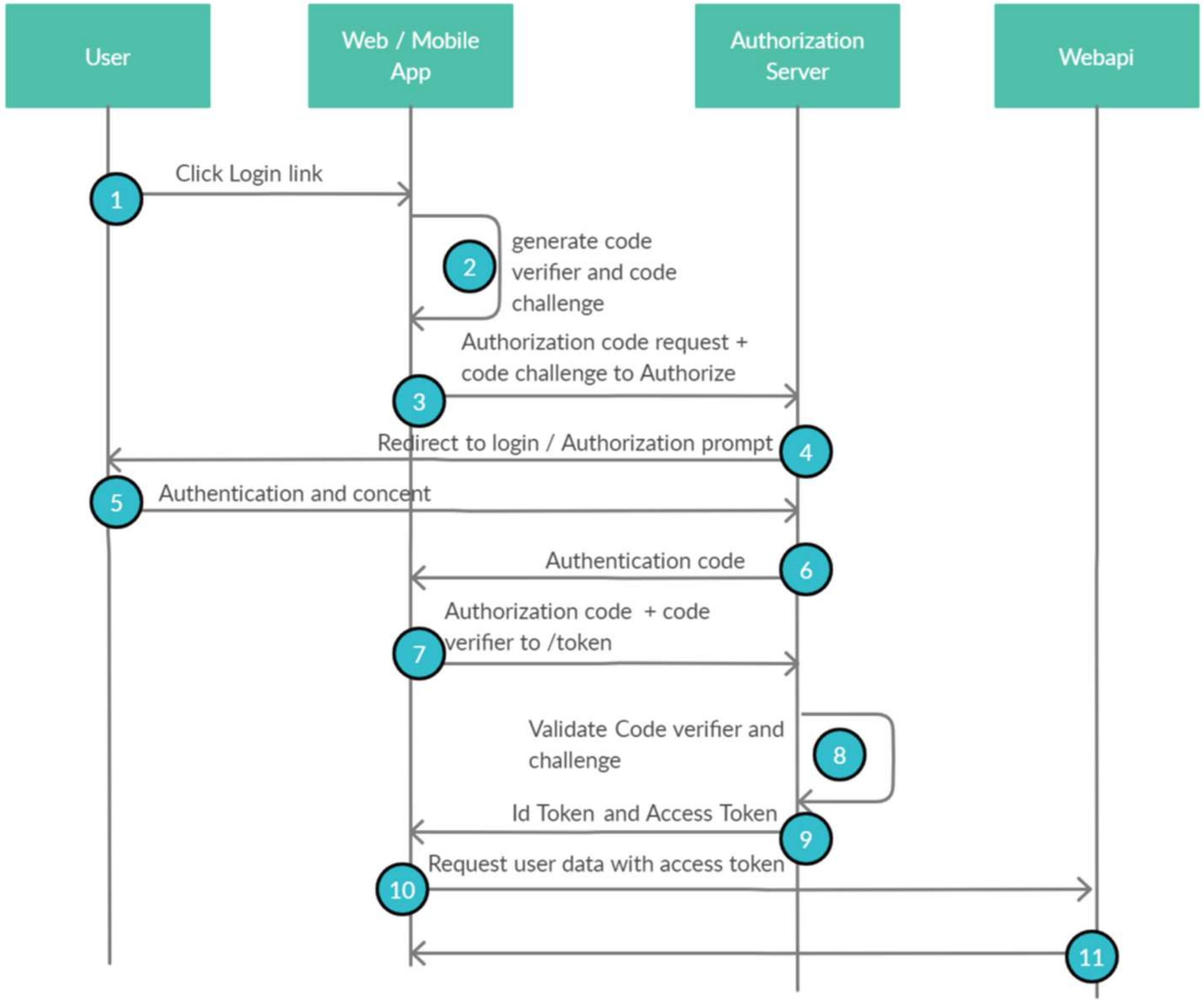
OAuth 2.0

- → Resource Owner
- → Resource Server
- → Authorization Server
- → Client application

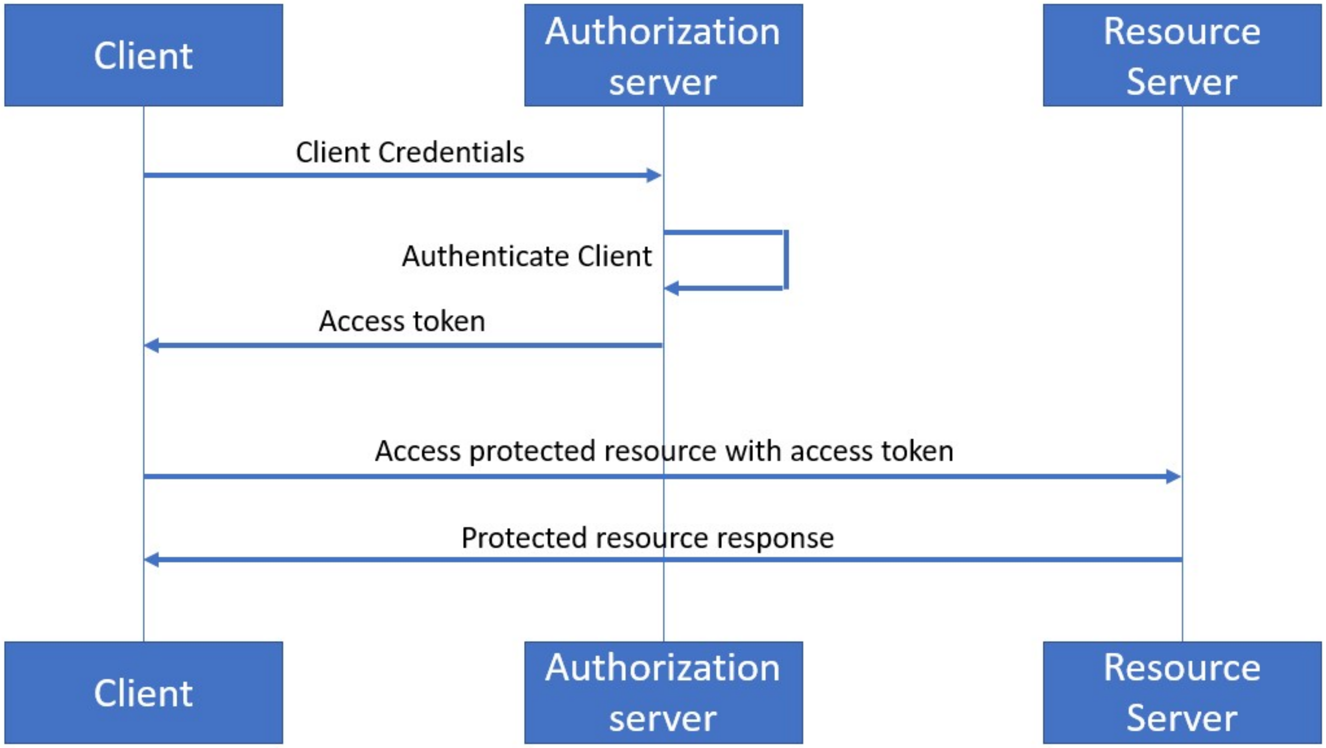
OAuth2.0 Auth_code



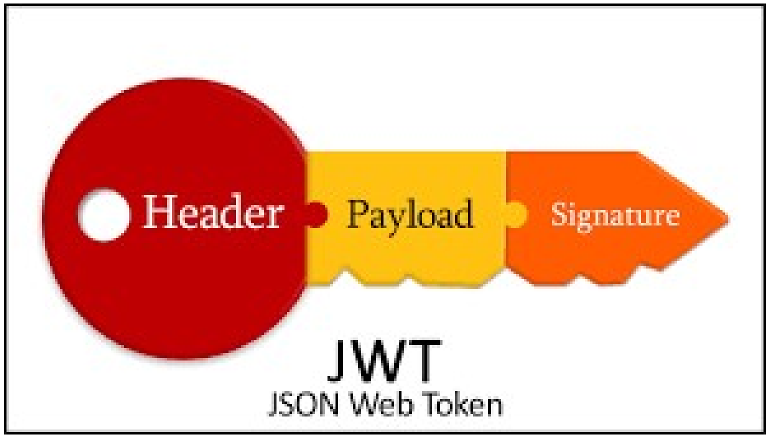
OAuth2.0 PKCE


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

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