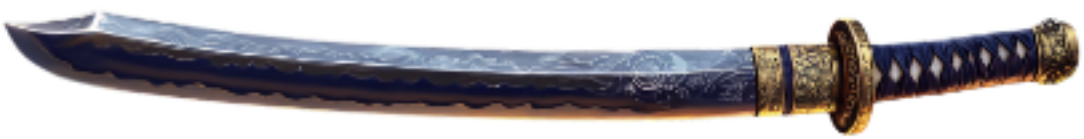
Web Apps

Authorization Code Flow



Properties:

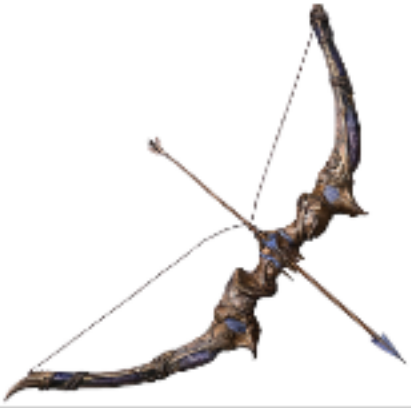
- Two-step exchange
- Secure backend channel for tokens
- Tokens never exposed to the browser
- Supports confidential clients
- Supports refresh tokens

Recommended for:

- Web Applications with a Backend

Single Page Apps, Mobile

Authorization Code Flow w/PKCE



Properties:

- Code Verifier + Code Challenge
- Protects against code interception
- Secure for public clients
- Works without client secrets
- Supports refresh tokens

Recommended for:

- Single Page Apps, Mobile Apps, Public Clients

Service Apps

Client Credentials Flow

Properties:

- No user involvement
- Direct client-to-server exchange
- Client secret required
- Service identity only (no user)
- No refresh tokens

Recommended for:

Server-to-Server, Background jobs

OpenID Connect

Properties:

- Returns signed JWT ID tokens
- Contains standardized user claims
- Provides UserInfo endpoint
- Supports discovery via well-known endpoints
- Facilitates single sign-on (SSO)
- Enables token validation without server calls

Recommended for:

- Single sign-on (SSO), Mobile and web app login

OpenID Connect

Properties:

- Returns signed JWT ID tokens
- Contains standardized user claims
- Provides UserInfo endpoint
- Supports discovery via well-known endpoints
- Facilitates single sign-on (SSO)
- Enables token validation without server calls

Recommended for:

- Single sign-on (SSO), Mobile and web app login

OAuth 2.1 - Auth Code Flow w/PKCE (“PIXIE” 🧚)

OAuth 2.1 - Auth Code Flow w/PKCE (“PIXIE” 🧚)