

OAuth 2.0 Best Practices





Use the Client Credentials grant for
machine-to-machine authorization



Use the Authorization Code grant
+ PKCE when a user is involved



Do not use the Password grant
Do not use the Implicit grant

Use Cases – Grant Types



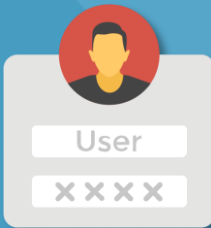
Web-server apps
authorization code + PKCE



Browser-based apps
~~implicit~~ authorization
code + PKCE



Mobile apps
~~implicit~~ authorization
code + PKCE



~~Username/Password access~~
password



Application access
client credentials



Always exactly match Redirect URIs
with the registered values



Use the HTTP Authorization header to pass access tokens to an API



Use Mutual TLS to authenticate clients and to enable sender-constrained access tokens



Refresh tokens must either be sender-constrained or one-time use