OAuth 2 Authorization
Authorization Code Flow

Client

Direct Resource Owner to Service Provider

A
Authenticate Resource Owner

Obtain Resource Owner Authorization

B
Direct Resource Owner to Client

Request Access Token

C
Validate Client

Validate Authorization Code

Exchange Access Code for Access Token

D
Grant Access Token

Service Provider

Obtain Authorization Code

A
Client sends Authorization Request

Request includes
response_type: token
client_id
redirect_uri (optional; may be pre-configured with service provider)
scope (optional)
state (recommended)

B
Service Provider grants Authorization

Redirection URI (302 Found) includes
code
state (required; IFF state was sent in the request; must be equal to what was received)

C
Client requests Access Token

Request includes
grant_type: authorization_code
code
redirect_uri (optional; may be pre-configured with service provider. Must match value sent in step A if provided)

D
Service Provider grants Access Token

(JSON response object (200 OK) includes
access_token
token_type
expires_in (optional)
refresh_token (optional)
scope (optional; SHOULD be included if the scope granted differs from the scope requested)

If the client is confidential, it must authenticate with the Authorization Server in this request.

©2012-The MITRE Corporation. All rights reserved.
OAuth 2 Authorization
Implicit Grant Flow

Client

Direct Resource Owner to Service Provider

A

Authenticate Resource Owner

Obtain Resource Owner Authorization

B

Direct Resource Owner to Client

Obtain Authorization Endpoint

Client sends
Authorization Request

Request includes
response_type: code
client_id
redirect_uri (optional; may be pre-configured with service provider)
scope (optional)
state (recommended)

Service Provider grants Authorization

Redirection URI (302 Found) includes (url-encoded in fragment)
access_token
token_type
expires_in (optional)
scope (optional)
state (required if state was sent in the request; must be equal to what was received)

Access Protected Resources
OAuth 2 Authorization
Resource Owner Password Credentials Flow

Client
- Outside the scope of this specification: Client obtains username and password credentials from the Resource Owner
  - Request Access Token
    - Validate Client
      - Validate Username and Password
        - Grant Access Token
          - Access Protected Resources

Service Provider
- Token Endpoint
  - Exchange Password Credentials for Access Token
    - Grant Access Token
      - Access Protected Resources

A
- Client requests Access Token
  - Request includes
    - grant_type: password
    - username
    - password
    - scope (optional)
  - If the client is confidential, it must authenticate with the Authorization Server in this request.

B
- Service Provider grants Access Token
  - JSON response object (200 OK) includes
    - access_token
    - token_type
    - expires_in (optional)
    - refresh_token (optional)
    - scope (optional; SHOULD be included if the scope granted differs from the scope requested)

©2012-The MITRE Corporation. All rights reserved.
**OAuth 2 Authorization**

**Client Credentials Flow**

Client

1. Client Authenticates with Authorization Server and Requests Access Token

Service Provider

A. Validate Client
   - Request includes
     - `grant_type: client_credentials`
     - `scope (optional)`
     - Client must authenticate with the Authorization Server in this request.

B. Service Provider grants Access Token
   - JSON response object (200 OK) includes
     - `access_token`
     - `token_type`
     - `expires_in (optional)`
     - `scope (optional; SHOULD be included if the scope granted differs from the scope requested)`

Access Protected Resources