OAuth 2 Authorization
Access Code Flow

Front Channel / Through User Agent

Back Channel / Direct Communication

Client

Service Provider

Direct User to Service Provider

A

Obtain User Authorization

B

Direct User to Consumer

Obtain Authorization Code

Authorization Endpoint

Request Access Token

C

Validate Client

Validate Authorization Code

D

Grant Access Token

Exchange Access Code for Access Token

Token Endpoint

Access Protected Resources

Access Protected Resources

A **Consumer 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
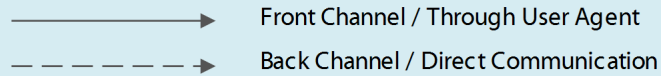state *(required IFF state was sent in the request; must be equal to what was received)*

C **Consumer 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)*

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

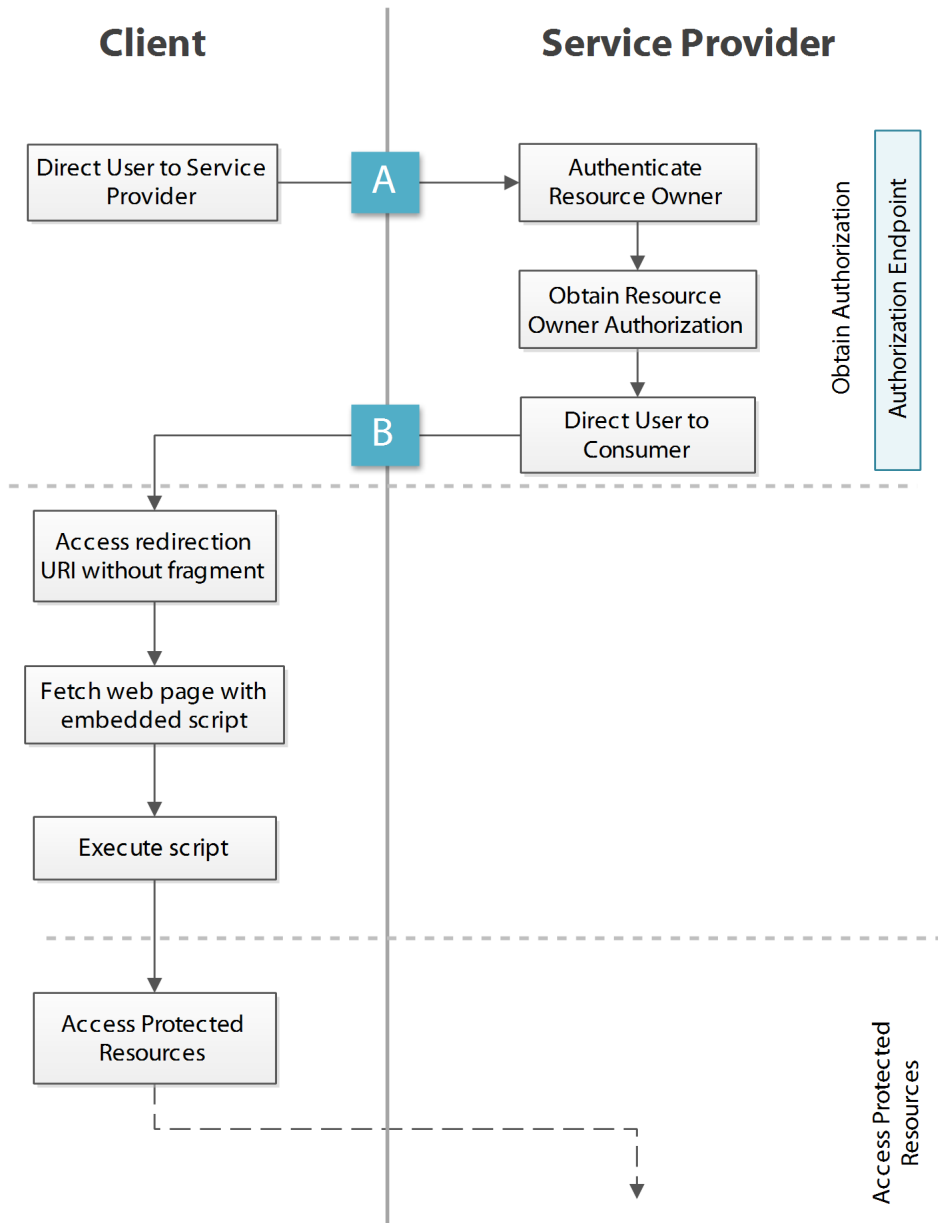**D** **Service Provider grants Access Token**

Response (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)*

Front Channel / Through User Agent

Back Channel / Direct Communication

Client

Service Provider

Direct User to Service Provider

A

Authenticate Resource Owner

Obtain Resource Owner Authorization

B

Direct User to Consumer

Obtain Authorization

Authorization Endpoint

Access redirection URI without fragment

Fetch web page with embedded script

Execute script

Access Protected Resources

Access Protected Resources

A Consumer sends **Authorization Request**

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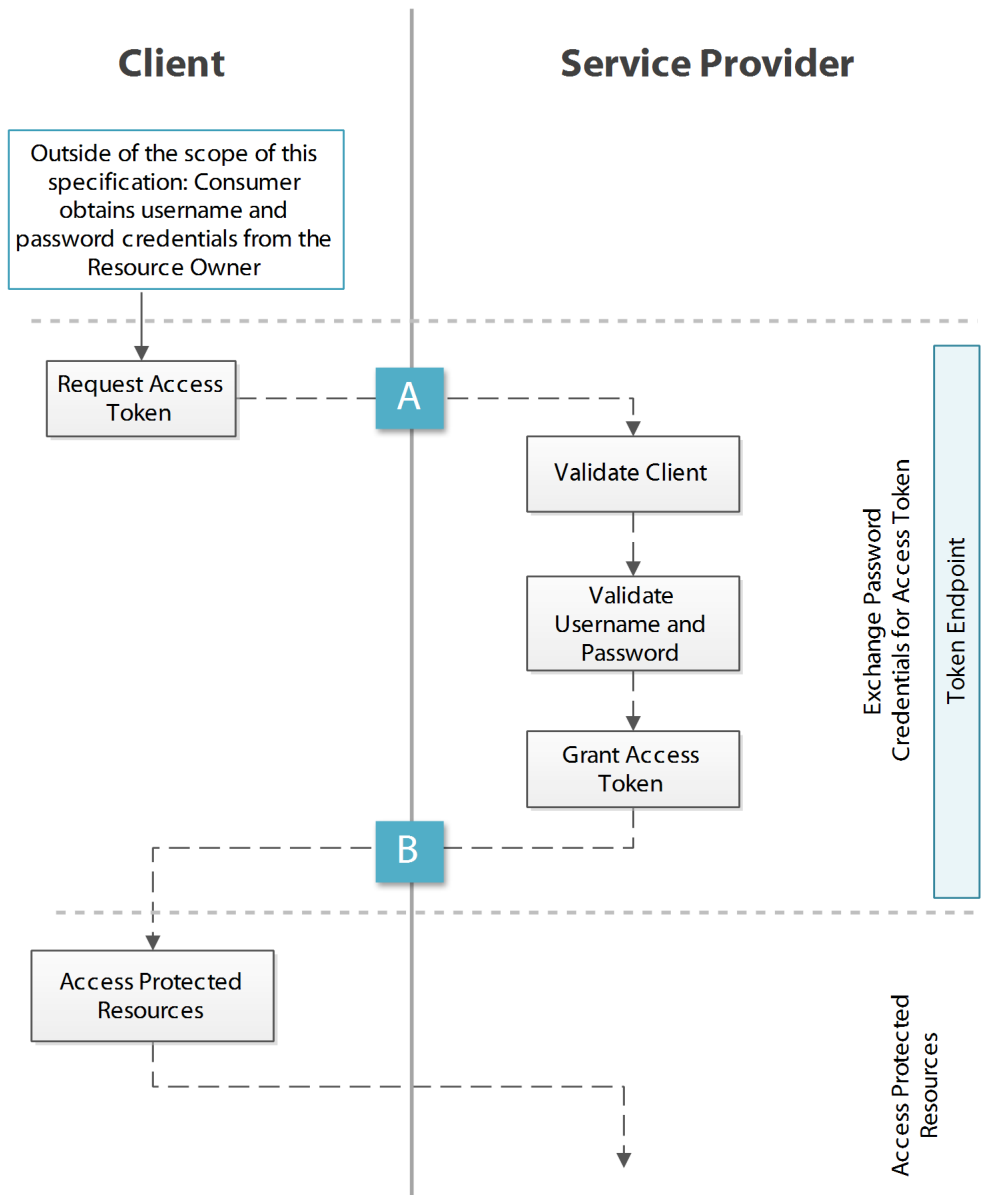scope *(optional)*
state *(recommended)*

B Service Provider grants **Authorization**

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

Client

Service Provider

Outside of the scope of this specification: Consumer obtains username and password credentials from the Resource Owner

Request Access Token

A

Validate Client

Validate Username and Password

Grant Access Token

Exchange Password Credentials for Access Token

Token Endpoint

B

Access Protected Resources

Access Protected Resources

A **Consumer requests Access Token**

Request includes
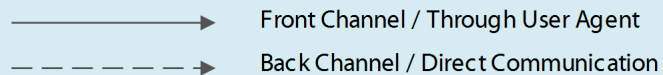grant_type: `password`
username
password
scope *(optional)*

If the client is confidential, it must authenticate with the Authorization Server in this request.
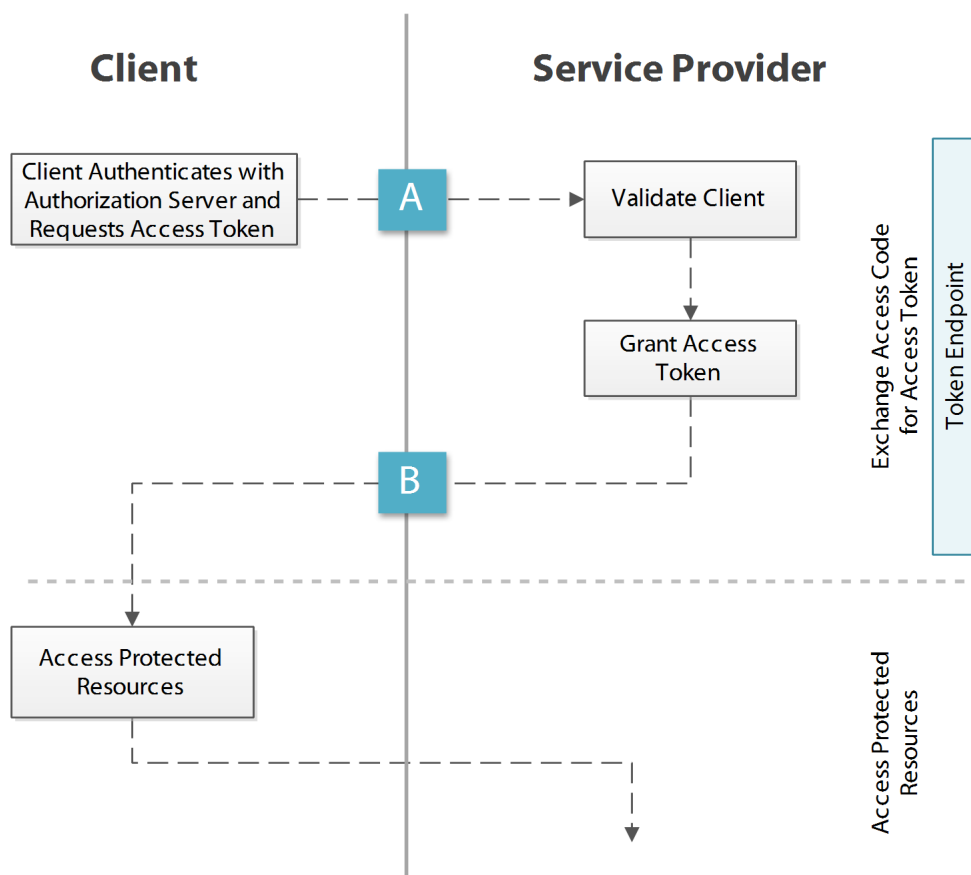
B **Service Provider grants Access Token**

Response (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)*

OAuth 2 Authorization
Client Credentials Flow

Client

Service Provider

Client Authenticates with Authorization Server and Requests Access Token

A

Validate Client

Grant Access Token

B

Exchange Access Code for Access Token

Token Endpoint

Access Protected Resources

Access Protected Resources

A **Consumer requests Access Token**

Request includes
grant_type: `client_credentials`
scope *(optional)*

Client must authenticate with the Authorization Server in this request.

B **Service Provider grants Access Token**

Response (200 OK) includes
access_token
token_type
expires_in *(optional)*
scope *(optional; SHOULD be included if the scope granted differs from the scope requested)*

Created by: Amanda Anganes