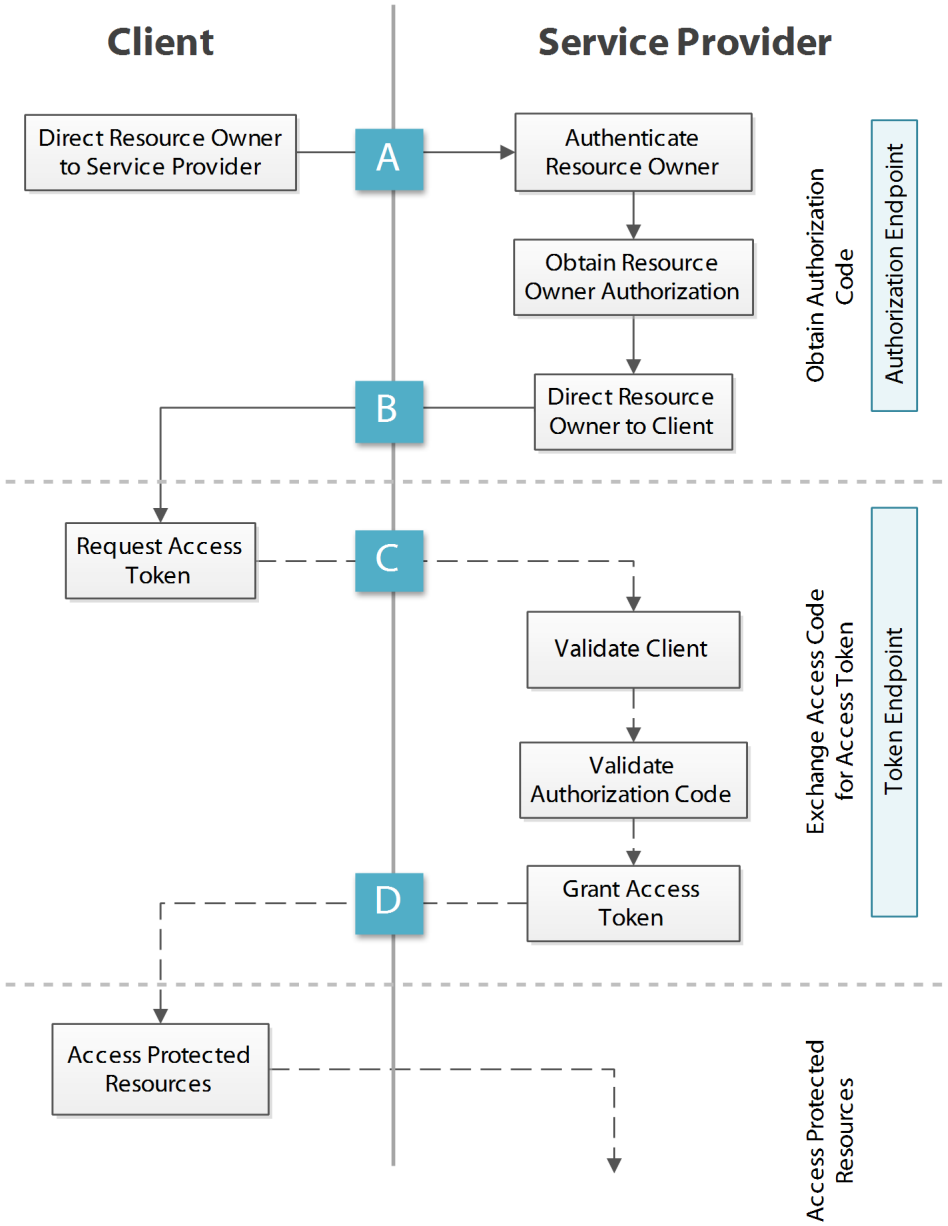
Front Channel / Through User Agent

Back Channel / Direct Communication

OAuth 2 Authorization

Authorization Code Flow



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)*

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

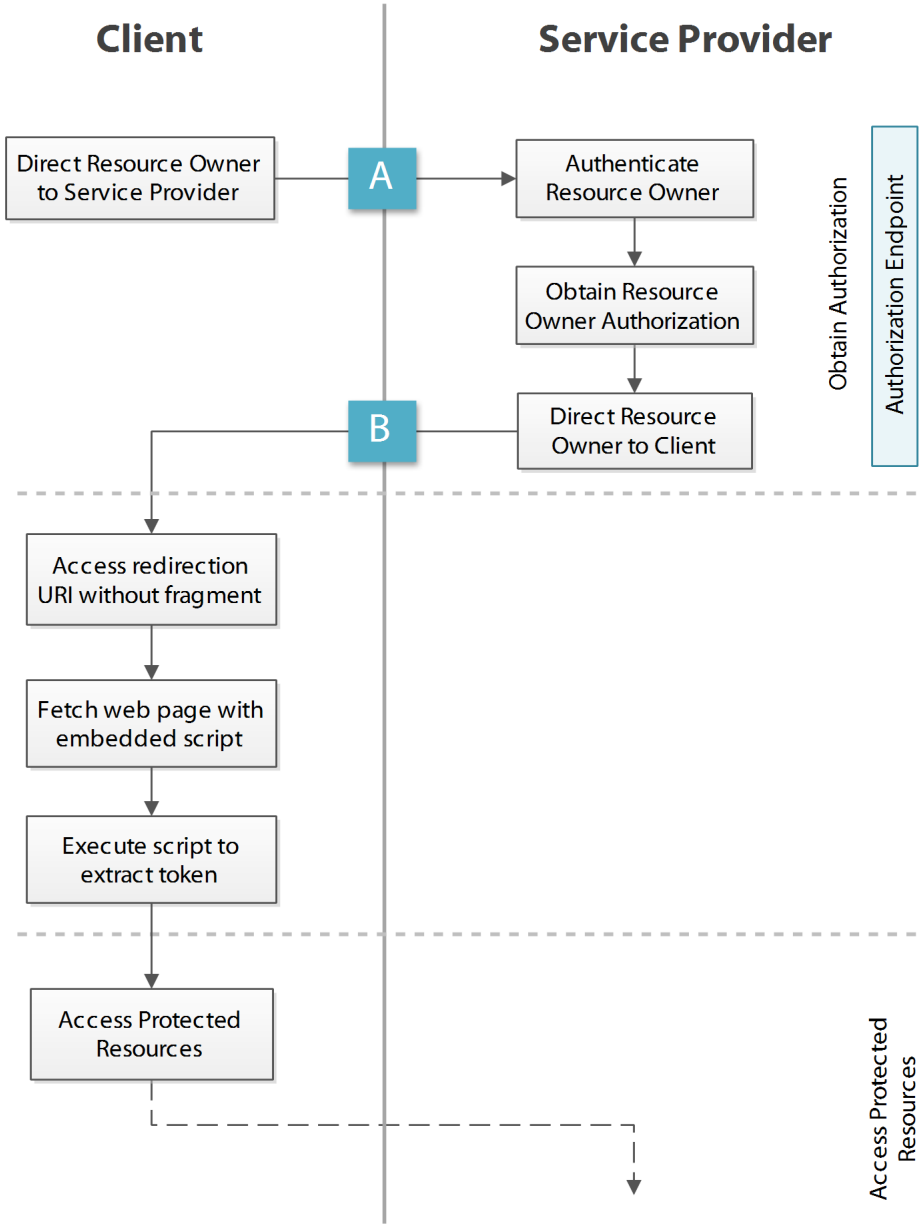
D **Service Provider grants Access Token**

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)*

Front Channel / Through User Agent

Back Channel / Direct Communication

OAuth 2 Authorization
Implicit Grant Flow



A

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)*

B

Service Provider grants Authorization

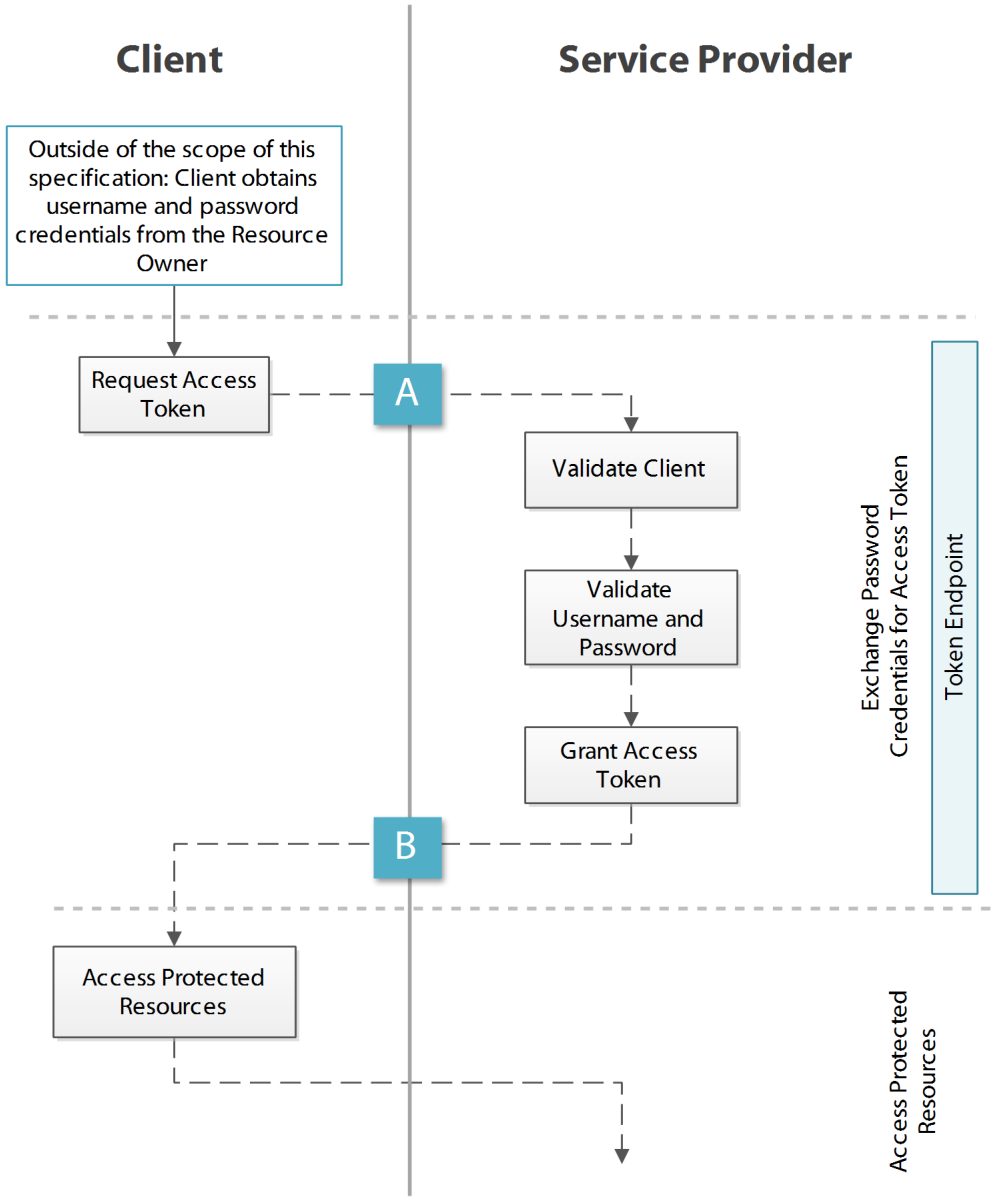
Redirection URI (302 Found) includes (url-encoded in fragment)
access_token
token_type
expires_in *(optional)*
scope *(optional)*
state *(required IFF state was sent in the request; must be equal to what was received)*

Front Channel / Through User Agent

Back Channel / Direct Communication

OAuth 2 Authorization

Resource Owner Password Credentials Flow



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**

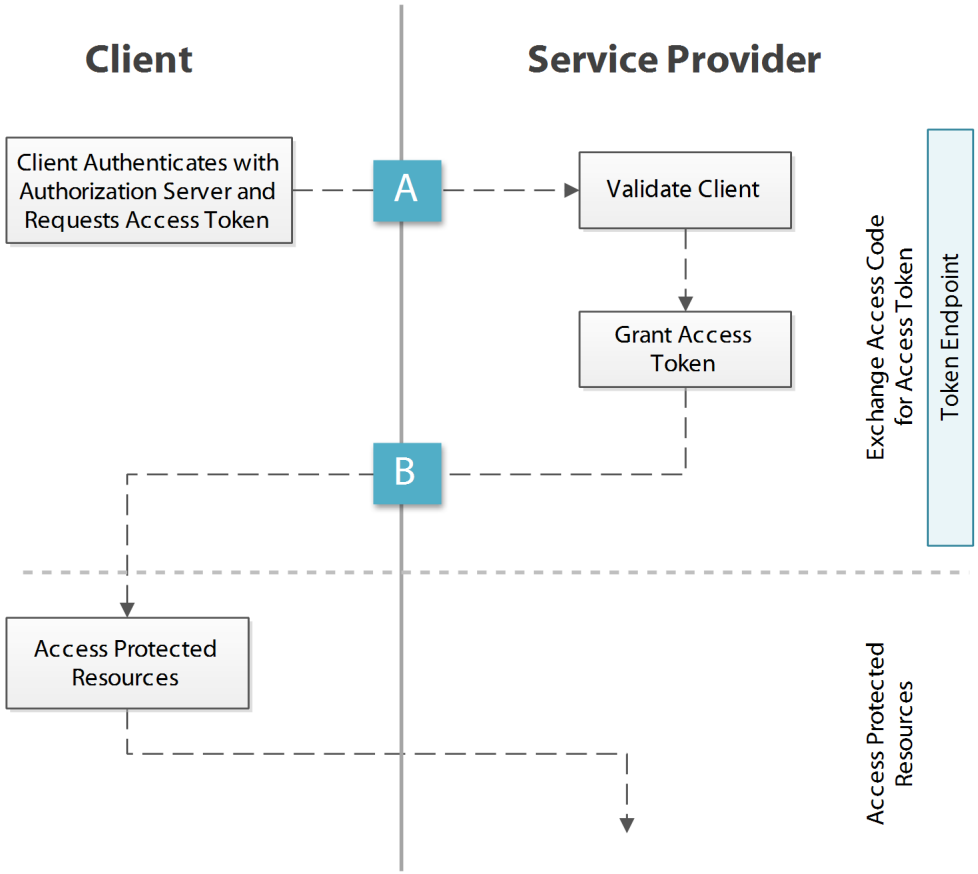
JSON response object (200 OK) includes
access_token
token_type
expires_in *(optional)*
refresh_token *(optional)*
scope *(optional; SHOULD be included if the scope granted differs from the scope requested)*

Front Channel / Through User Agent

Back Channel / Direct Communication

OAuth 2 Authorization

Client Credentials Flow



A **Client 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**

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)*

Approved for Public Release: 11-5233. Distribution Unlimited.

Created by: Amanda Anganes