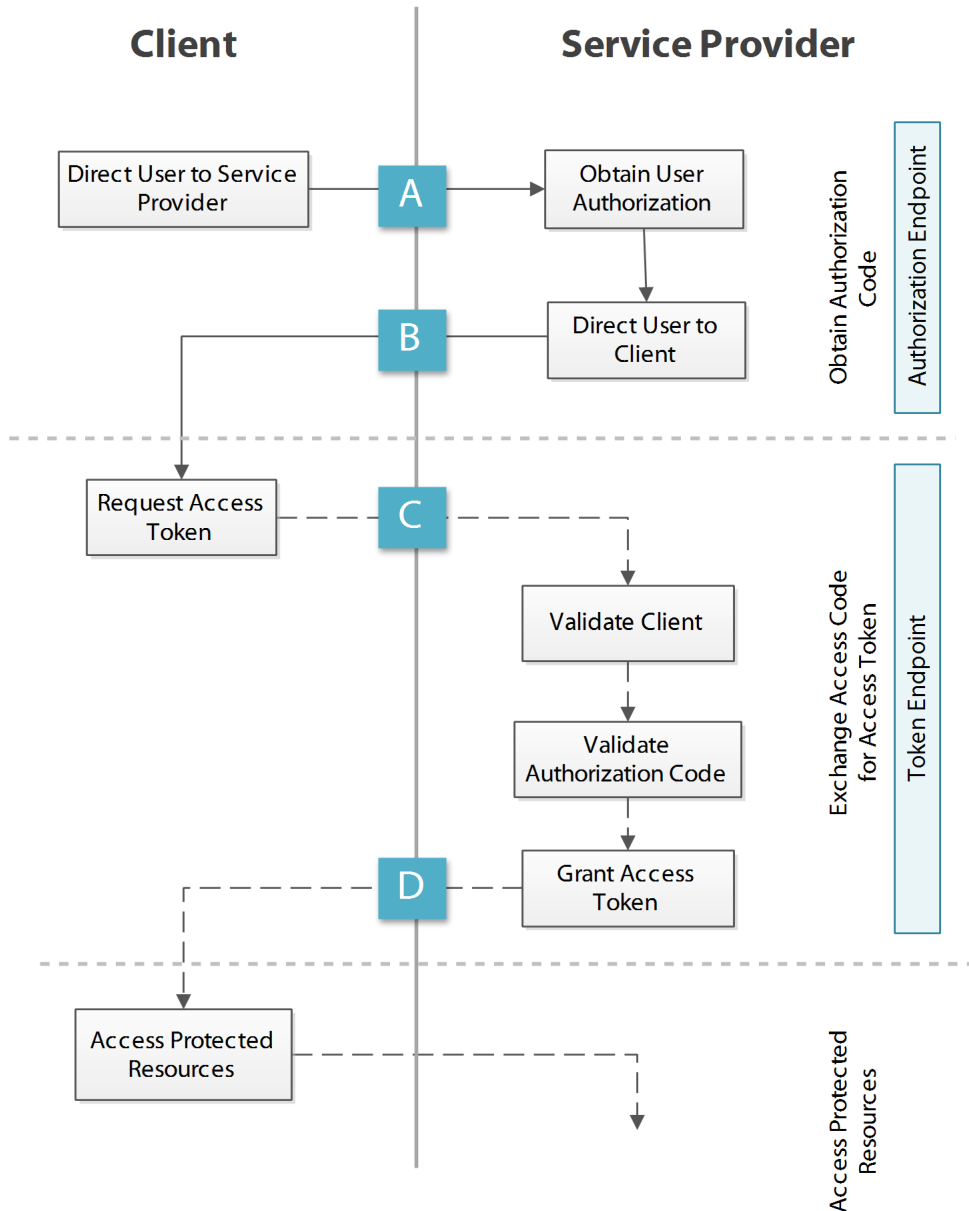


—————> Front Channel / Through User Agent  
 - - - - -> Back Channel / Direct Communication

# OAuth 2 Authorization

## Access 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)

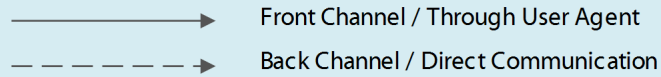
**C Client requests Access Token**

**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)

**D Service Provider grants Access Token**

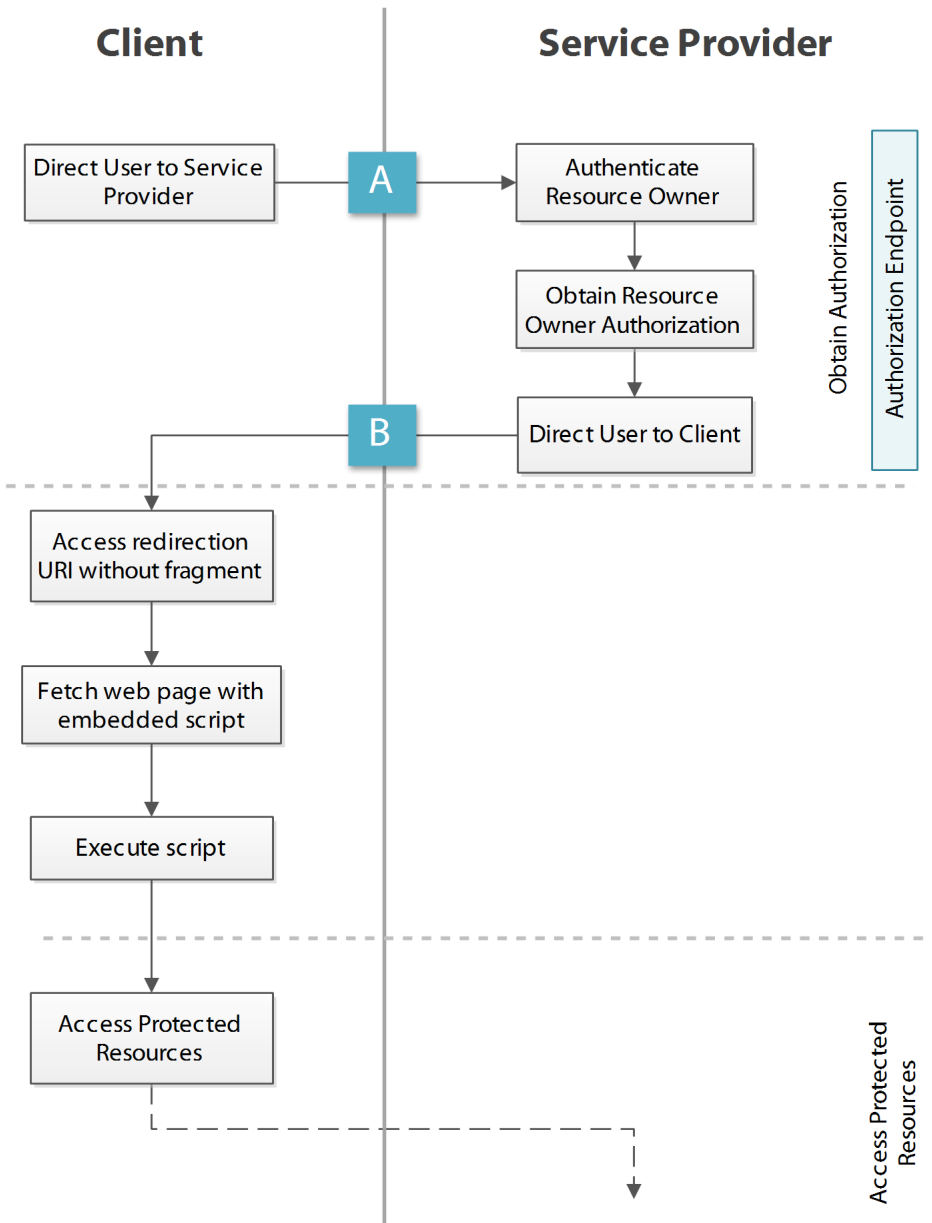
**Response (200 OK) includes**  
 access\_token  
 token\_type  
 expires\_in (optional)  
 refresh\_token (optional)  
 scope (optional; SHOULD be included if the scope granted differs from the scope requested)

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



# 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)

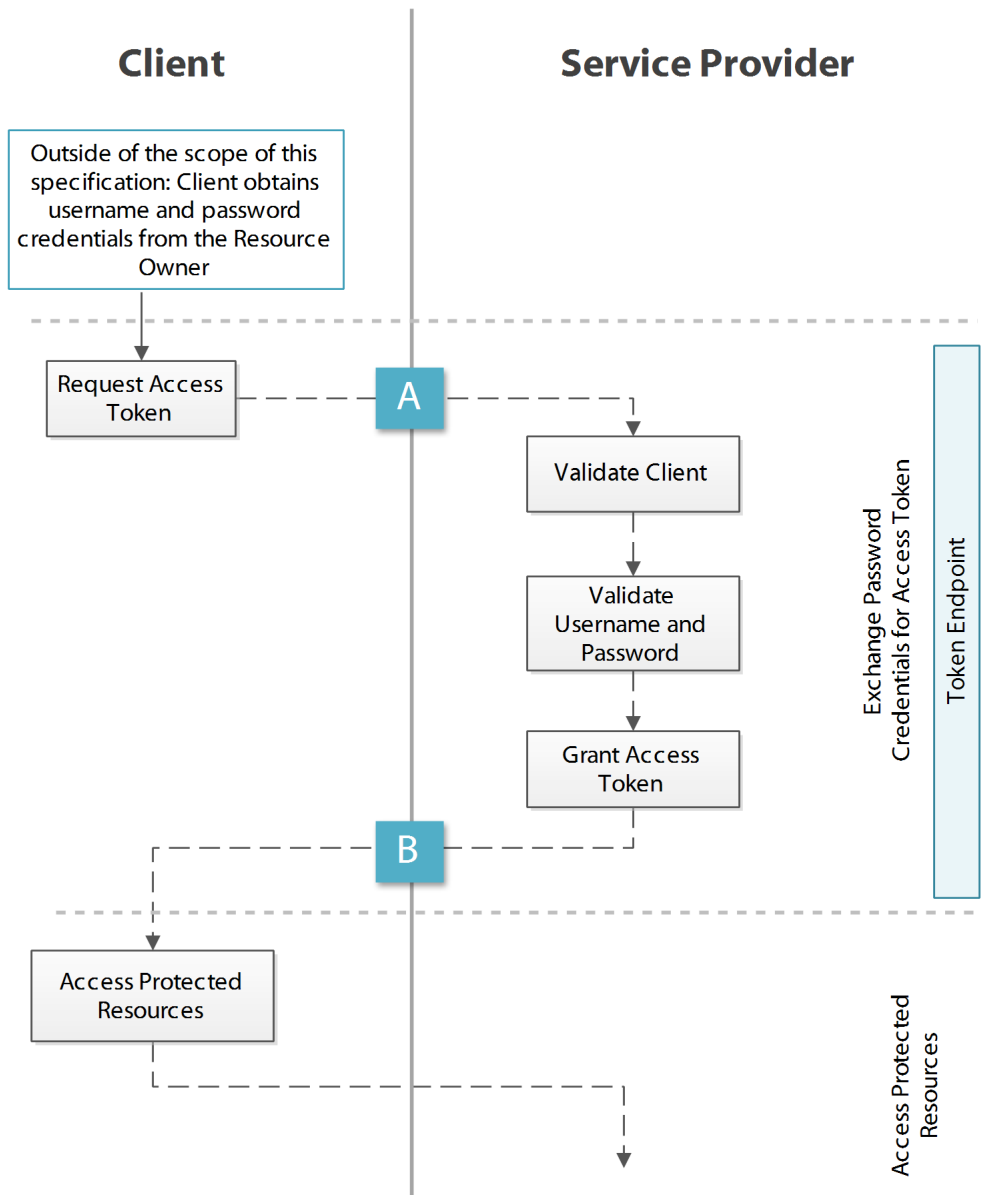
**B** Service Provider grants **Authorization**

**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)

# OAuth 2 Authorization

## Resource Owner Password Credentials Flow

—————> Front Channel / Through User Agent  
 - - - - -> Back Channel / Direct Communication



### 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.**

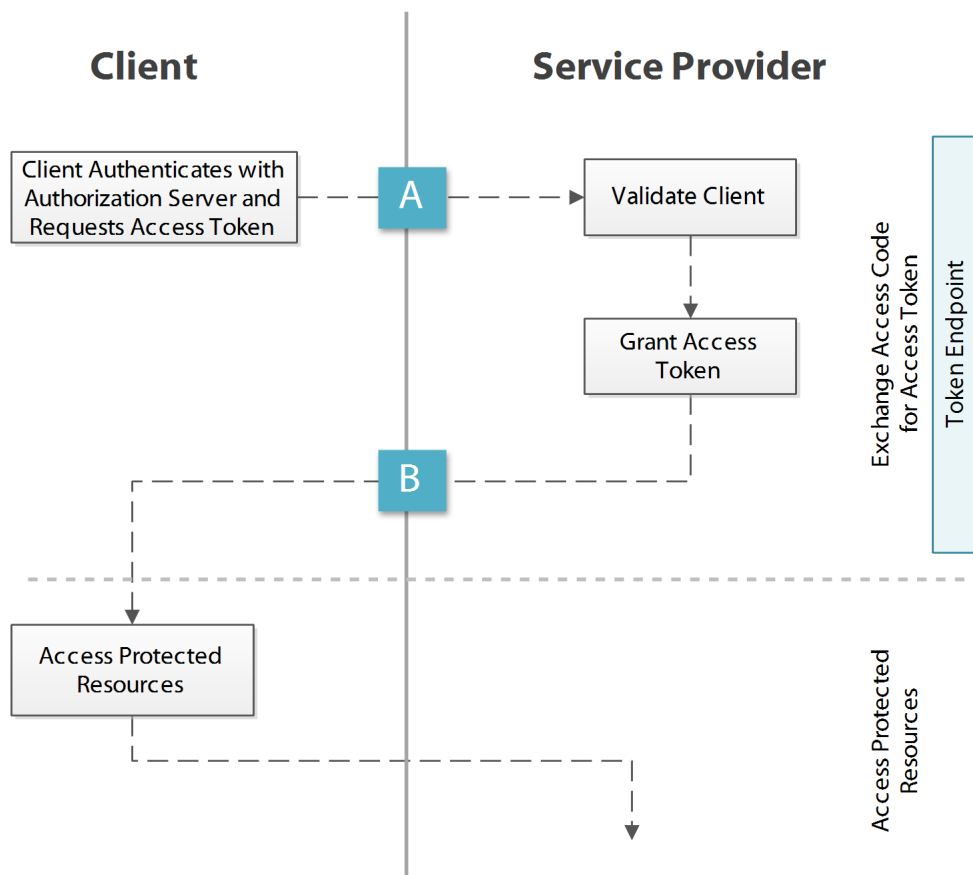
### B Service Provider grants Access Token

#### 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

# 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**

**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)

©2012-The MITRE Corporation. All rights reserved.

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

Created by: Amanda Anganes