4.3. 资源所有者密码凭据许可(4.3. Resource Password Credentials Grant)

4.3. 资源所有者密码凭据许可

[illegible] 只有 [illegible] 接身份验证方案的客户端至OAu

```
+----------+
| Resource |
|  Owner   |
|          |
+----------+
     v
     |    Resource Owner
    (A) Password Credentials
     |
     v
+---------+                                  +---------------+
|         |>--(B)---- Resource Owner ------->|               |
|         |         Password Credentials     | Authorization |
| Client  |                                  |     Server    |
|         |<--(C)---- Access Token ---------<|               |
|         |    (w/ Optional Refresh Token)   |               |
+---------+                                  +---------------+
```

图5：资源所有者密码凭据流程

图5中的所示流程包含以下步骤：

- (A) 资源所有者提供给客户端它的用户名和密码。
- (B) 通过包含从资源所有者处接收到的凭据，客户端从授权服务器的令牌端点请求访问令牌。当发起请求时，客户端与授权服务器进行身份验证。
- (C) 授权服务器对客户端进行身份验证，验证资源所有者的凭证，如果有效，颁发访问令牌。

4.3. Resource Owner Password Credentials

Grant

The resource owner password credentials grant type is suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged

---

application. The authorization server should take special care when enabling this grant type and only allow it when other flows are not viable.

This grant type is suitable for clients capable of obtaining the resource owner's credentials (username and password, typically using an interactive form). It is also used to migrate existing clients using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token.

```
     +----------+
     | Resource |
     |  Owner   |
     |          |
     +----------+
          v
          |    Resource Owner
         (A) Password Credentials
          |
          v
     +---------+                                  +---------------+     |         |>--(B)----
Resource Owner ------->|               |     |         |        Password Credentials     |
Authorization |
     | Client  |                                  |     Server    |     |         |<--(C)----
Access Token ---------<|               |     |         |    (w/ Optional Refresh Token)
|               |
     +---------+                                  +---------------+
            Figure 5: Resource Owner Password Credentials Flow
   The flow illustrated in Figure 5 includes the following steps:
   (A)  The resource owner provides the client with its username and
        password.
   (B)  The client requests an access token from the authorization        server's token
endpoint by including the credentials received        from the resource owner.  When making the
request, the client
        authenticates with the authorization server.
   (C)  The authorization server authenticates the client and validates        the resource
owner credentials, and if valid, issues an access
        token.
```

Revision #1
Created Wed, Mar 25, 2020 10:55 PM by 爱异常
Updated Wed, Mar 25, 2020 10:56 PM by 爱异常