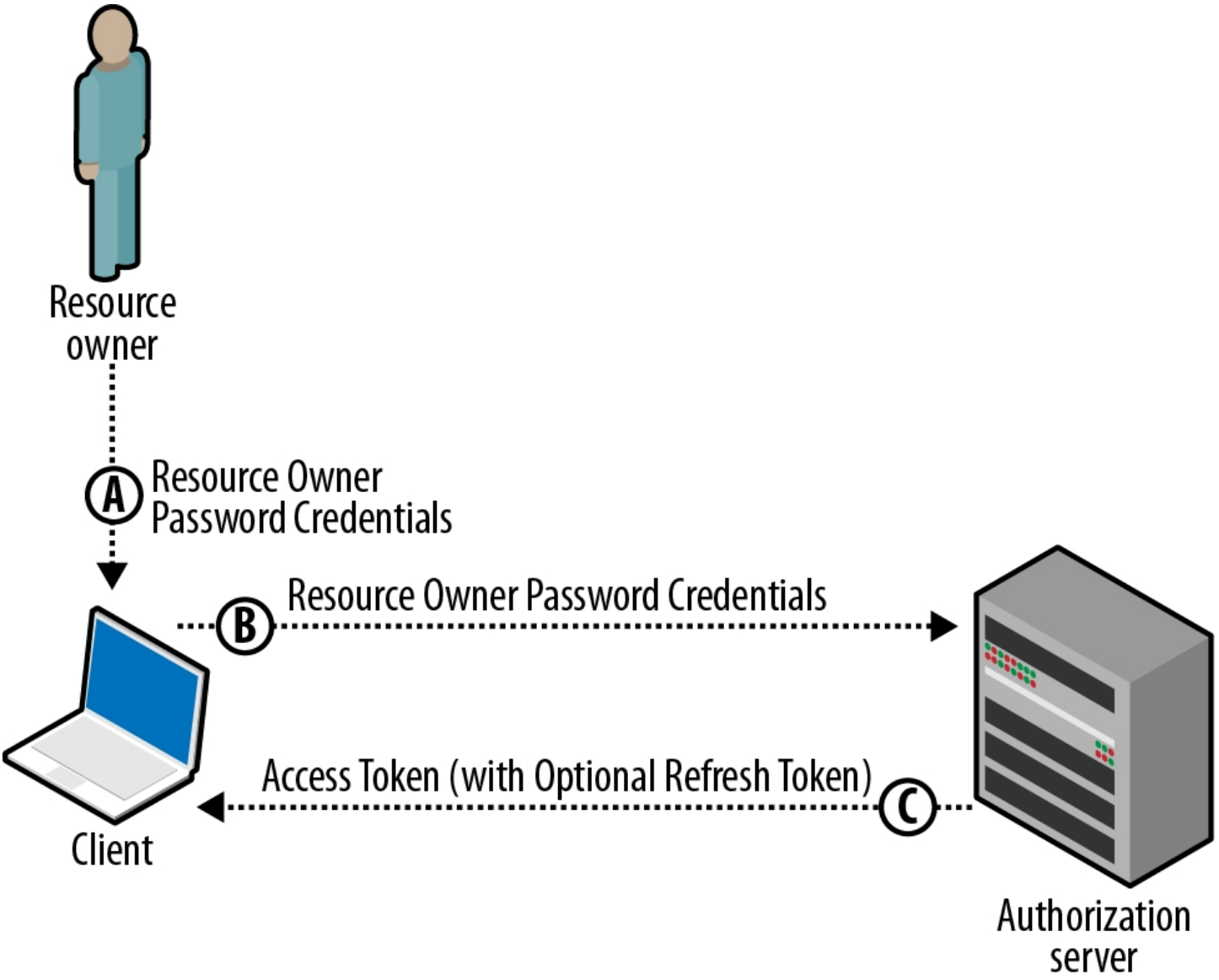
适用范围

这种模式会直接将用户密码暴露给应用程序，因此应谨慎使用。一般说来，只有信任度极高的客户才应授权使用该模式，如官方移动应用、操作系统或高权限程序。

流程剖析



为了阐述该授权类型的认证过程，我们以Salesforce中基于REST的API为例进行说明。

1. 向用户索要认证信息

首先，我们必须得让用户将认证信息提供给应用程序。对于Salesforce来说，如果用户处于不可信的网络中时，除了需要输入用户名和密码外，还需要用户提供一个安全令牌作为用户的第三个输入。

2. 交换访问令牌

这里的访问令牌交换过程与授权码类型的验证授权（authorization code）很相似。我们要做的就是向认证服务器提交一个POST请求并在其中提供相应的认证和客户信息。

你可以通过查阅API文档得到认证服务器的URL，如Salesforce的URL为：

https://login.salesforce.com/services/oauth2/token

下面是所需的POST参数：

grant_type

该模式下为“password”

scope

业务访问控制范围，这在Salesforce中是不需要的，但对其其他的API来说则是一个可选参数

client_id

应用注册时获得的客户id

client_secret

应用注册时获得的客户密钥

username

用户的用户名，以UTF-8编码

password

用户的密码，以UTF-8编码。对于Salesforce，还需将安全令牌串连起来。

以下是一个通过命令行HTTP客户端curl发起的请求示例：

```
curl -d "grant_type=password" \
-d "client_id=3MVG9QDx8IKCsXTFM0o9aE3KfEwsZLvRt" \
-d "client_secret=4826278391389087694" \
-d "username=ryan%40ryguy.com" \
-d "password=_userspassword__userssecuritytoken_" \
https://login.salesforce.com/services/oauth2/token
```

如果用户提供的认证信息正确，则Salesforce的OAuth认证服务器会返回一段application/json数据并包含access_token：

```
{
    "id":"https://login.salesforce.com/id/00DU0000000Io8rMAC/005U0000000hMDCIA2",
    "issued_at":"1316990706988",
    "instance_url":"https://na12.salesforce.com",
    "signature":"Q2KTt8Ez5dwJ4Adu6QttAhCxbEP3HyfaTUXoNI=",
    "access_token":"00DU0000000Io8r!AQcKbNiJPt0OCSAvxU2SBjVGP6hW0mfmKH07QiPEGIX"
}
```

这些响应参数有什么含义呢？

access_token

用于访问API接口的访问令牌。这是该响应中唯一需要的内容

id（Salesforce中的特有项）

用户的唯一身份

instance_url

访问API时的URL前缀

signature

一个签名，用于验证URL在传输过程中没有被篡改

issued_at（Salesforce中的特有项）

签名生成的时间，用于验证

3. 访问API

仅以一个示例作为演示：

```
curl -d "q=SELECT+name+FROM+Account"\
-H 'Authorization: Bearer 00DU0000000Io8r!AQcAQKJ.Cg1dCBCVHmx2.Iu3lroPQBV2P65_jXk'
```