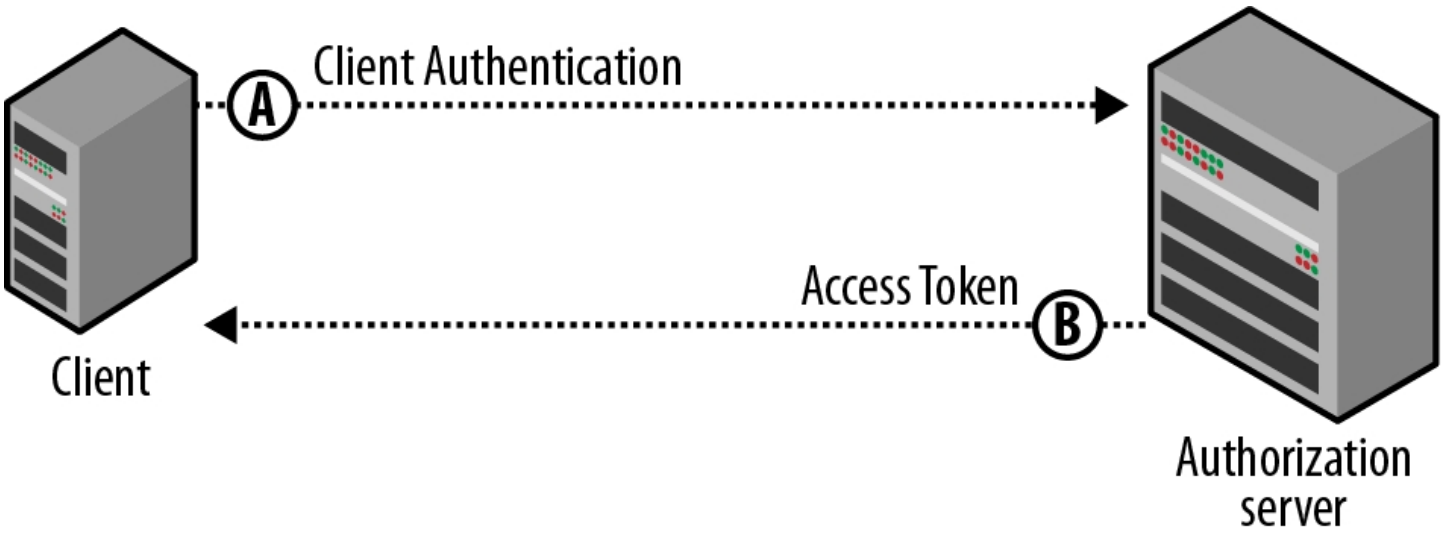
适应范围

认证服务器不提供像用户数据这样的重要资源，仅仅是有限的只读资源或者一些开放的API。例如使用了第三方的静态文件服务，如Google Storage或Amazon S3。这样，你的应用需要通过外部API调用并以应用本身而不是单个用户的身份来读取或修改这些资源。这样的场景就很适合使用客户端证书授权。

流程剖析



1. 用客户端证书交换访问令牌

应用程序需要向认证服务器申请访问令牌，而该请求则需要客户端证书进行认证。

假设现在我们正在折腾facebook，其认证URL为：

https://graph.facebook.com/oauth/access_token

这里需要使用POST请求并附带以下参数：

grant_type

这里为“client_credentials”

client_id

应用注册时获得的client id

client_secret

应用注册时获得的client secret

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=client_credentials\
&client_id=201627111111111117128396\
&client_secret=904b98aaaaaaac1c92381d2" \
https://graph.facebook.com/oauth/access_token
```

如果认证成功，服务器将会返回access_token：

```
{
    "access_token":"201627111111111117128396|8VG0riNauEzttXkUXBtUbw"
}
```

2. 访问API

到这里就毫无疑问了，你只需通过HTTP Authorization头或查询参数提供获取到的access_token即可正常访问API，具体要以何种形式传递access_token则取决于API提供商的支持。

以下是用curl发起的API请求并以查询参数的形式传递access_token：

```
curl "https://graph.facebook.com/202627763128396/insights?\
access_token=201627111111111117128396|8VG0riNauEzttXkUXBtUbw"
```