

# 第07期-混合授权模式组合授权

2020年6月15日 9:24

## 为什么要把访问令牌和身份令牌分开返回呢？

### 身份认证与授权，OpenID Connect 与 OAuth 2.0，身份令牌与访问令牌

access token 不含有任何关于身份认证的信息（用户声明信息），access token 的生命期可能会非常的长，即使用户离开了它仍有可能有效，它还有可能被用于无最终用户参与的情况，还有一种情况就是 access token 可能会被其它的客户端应用借用。

所以，无论客户端是如何得到的 access token, 它都无法从 access token 里得到最终用户的信息以及最终用户的身份认证状态（用户声明信息）。

在 OAuth2.0 里，access token 不是为客户端准备的，它对于客户端应该是不透明的，但是客户端也需要从 access token 得到一些用户信息，实际上客户端应用只是 access token 的展示者，access token 真正的目标观众是被保护的资源。

在 OpenID Connect 里，加了一个 ID Token 令牌，它会和 access token 一同发送给客户端应用，用于识别当前用户是他声称的用户。

<https://www.cnblogs.com/cqzl/p/9231219.html>

## Identityserver 混合授权模式

```
AllowedGrantTypes = GrantTypes.Hybrid
```

```
options.ResponseType = OpenIdConnectResponseType.CodeIdToken
```

## 授权码code模式跳转参数

```
response_type=code
```

## 隐式简化 Implicit 模式参数

```
response_type=id_token  
response_type=token  
response_type=id_token token
```

## Hybrid 混合模式

response\_type=code id\_token  
response\_type=code token  
response\_type=code id\_token token

以 response\_type=code id\_token 为例说明

