## **定义身份资源**

身份资源是用户的用户ID，名称或电子邮件地址等数据。标识资源具有唯一名称，您可以为其分配任意声明类型。然后，这些声明将包含在用户的身份令牌中。

OpenID Connect规范指定了几个[标准](https://openid.net/specs/openid-connect-core-1_0.html" \l "ScopeClaims)身份资源。最低要求是，您为用户发送唯一ID提供支持 。这是通过公开名为的标准身份资源来完成的openid：

**public** **static** IEnumerable<IdentityResource> GetIdentityResources(){

**return** **new** List<IdentityResource>

{

**new** IdentityResources.OpenId()

};}

## **定义自定义标识资源**

您还可以定义自定义标识资源。创建一个新的IdentityResource类，为其命名，并可选择显示名称和描述，并定义在请求此资源时应将哪些用户声明包含在身份令牌中：

**public** **static** IEnumerable<IdentityResource> GetIdentityResources()

{

var customProfile = **new** IdentityResource(

name: "custom.profile",

displayName: "Custom profile",

claimTypes: **new**[] { "name", "email", "status" });

**return** **new** List<IdentityResource>

{

**new** IdentityResources.OpenId(),

**new** IdentityResources.Profile(),

customProfile

};}

## **定义API资源**

要允许客户端请求API的访问令牌，您需要定义API资源，例如：

要获取API的访问权限，您还需要将它们注册为范围。这次范围类型是Resource类型：

**public** **static** IEnumerable<ApiResource> GetApis(){

**return** **new**[]

{

*// simple API with a single scope (in this case the scope name is the same as the api name)*

**new** ApiResource("api1", "Some API 1"),

*// expanded version if more control is needed*

**new** ApiResource

{

Name = "api2",

*// secret for using introspection endpoint*

ApiSecrets =

{

**new** Secret("secret".Sha256())

},

*// include the following using claims in access token (in addition to subject id)*

UserClaims = { JwtClaimTypes.Name, JwtClaimTypes.Email },

*// this API defines two scopes*

Scopes =

{

**new** Scope()

{

Name = "api2.full\_access",

DisplayName = "Full access to API 2",

},

**new** Scope

{

Name = "api2.read\_only",

DisplayName = "Read only access to API 2"

}

}

}

};}