

Understanding Identity: OpenID Connect



Kevin Dockx

@KevinDockx | <http://blog.kevindockx.com/>

We Have an Issue...



If OAuth 2.0 is about authorization, how do we handle authentication? And how do we get identity-related information?



OpenID Connect 1.0 is a simple
identity layer on top of the OAuth
2.0 protocol

OpenID Connect

Core functionality:

Authentication

Claims about the user

It's built on top of OAuth 2.0

(so we can still use what we've learned about authorization)

Ref: http://openid.net/specs/openid-connect-core-1_0.html



```
{  
  "sub": "b05d3546-6ca8-4d32-b95c-77e94d705ddf",  
  "amr": "password",  
  "auth_time": 1443100792,  
  "idp": "idsrv",  
  "given_name": "Kevin",  
  "family_name": "Dockx",  
  "iss": "https://tripcompanysts/identity",  
  "aud": "tripgalleryhybrid",  
  "exp": 1443101095,  
  "nbf": 1443100795  
}
```

OpenID Connect



id_token contains claims about the authentication of an end user (and potentially other requested claims)

id_tokens can be used for signing in to an application. Access tokens are for accessing resources!

UserInfo endpoint

- can be used by the client to get more user information of the authenticated user
- these claims are requested with the **access_token**

OpenID Connect Flows

OpenID Connect extends OAuth 2.0's Authorization Code and Implicit flows

Authorization Code

Implicit

... and introduces a new one

Hybrid

Scopes and Claims

OpenID Connect adds **identity** scopes to OAuth 2.0's resource scopes

profile scope

name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, updated_at

email scope

email, email_verified

address scope

address

phone scope

phone_number, phone_number_verified

Summary



OpenID Connect adds **authentication & identity information**

It introduces the **UserInfo** endpoint

It extends the Authorization Code and Implicit flows, and introduces a new one: the **Hybrid** flow

Identity scopes relate to a set of claims