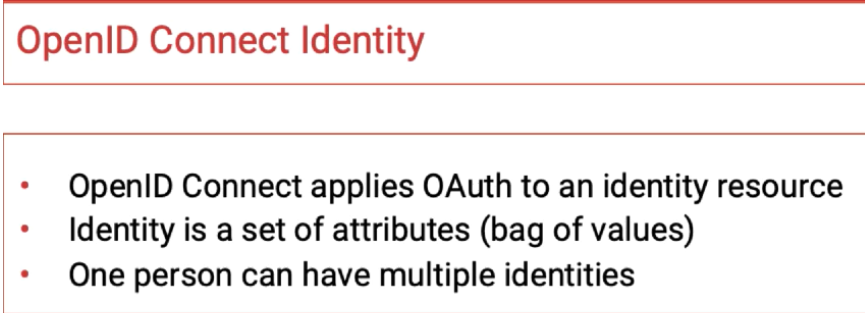


1. This means anyone with ACCESS TOKEN can be authorized, cannot identify if the user issuing the ACCESS TOKEN is actual owner of the resource



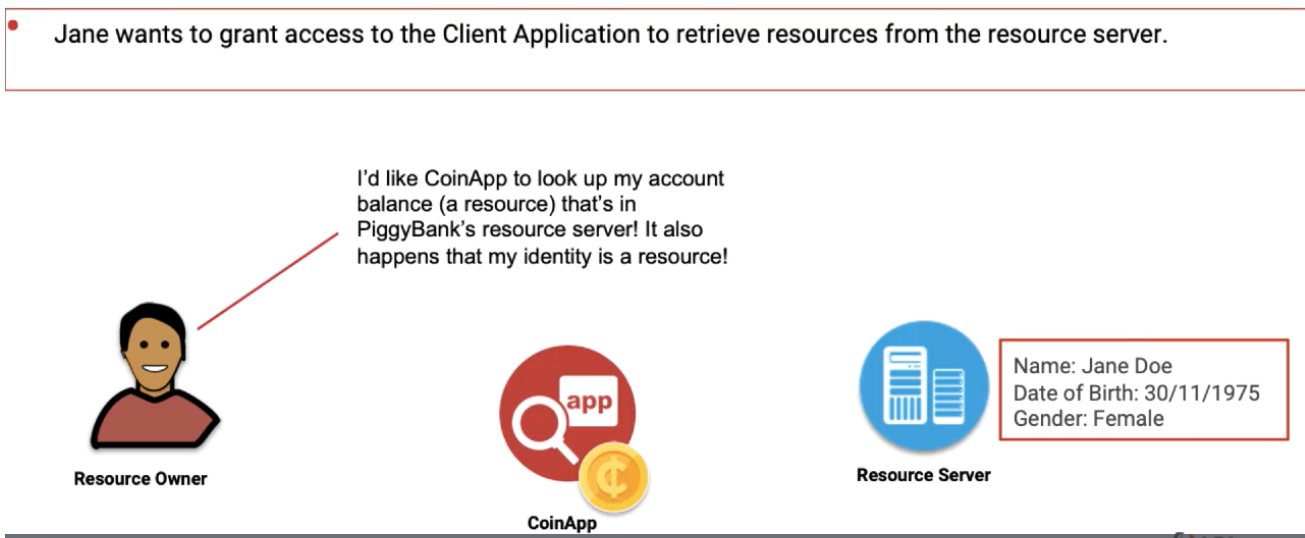
If OpenID is included in the scope, ID TOKEN will be issued along with ACCESS TOKEN



ID TOKEN acts like encrypted fingerprint

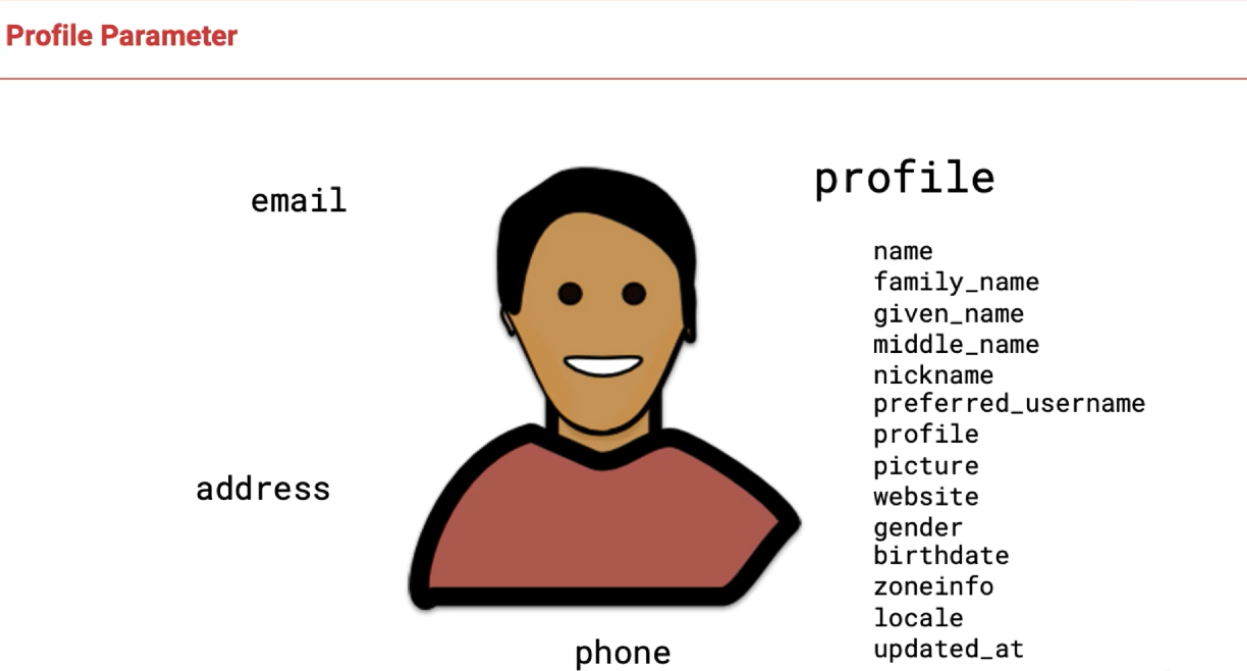
ID TOKEN can be decoded to reveal user information for identity verification

**User\_info endpoint** can also be used to reveal user information

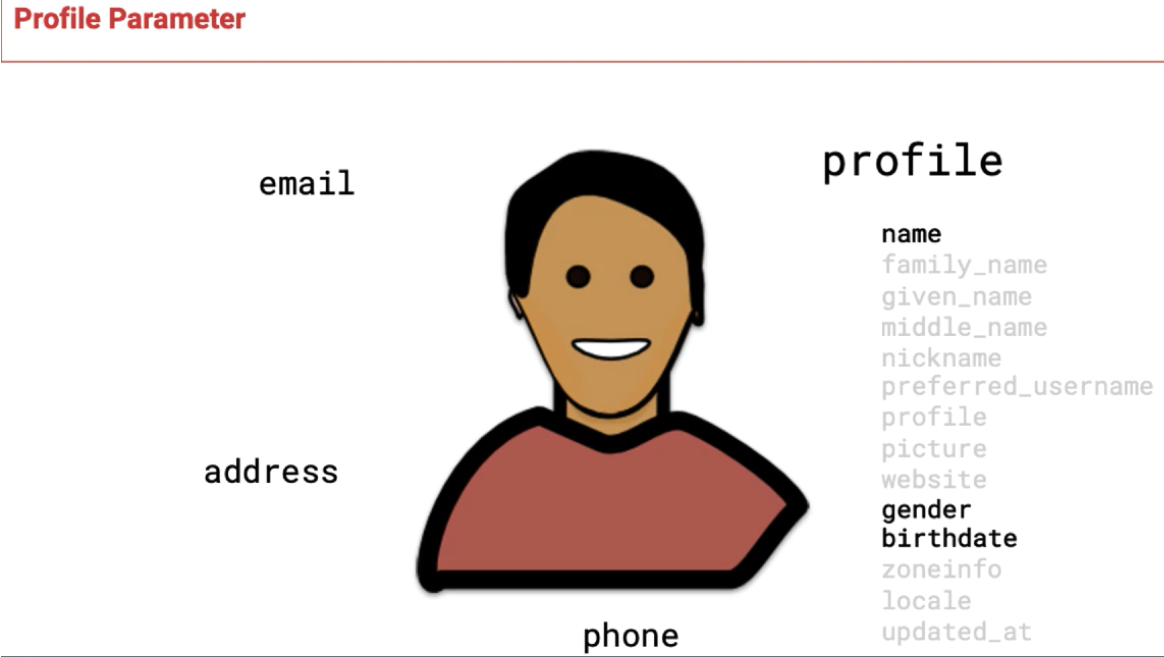




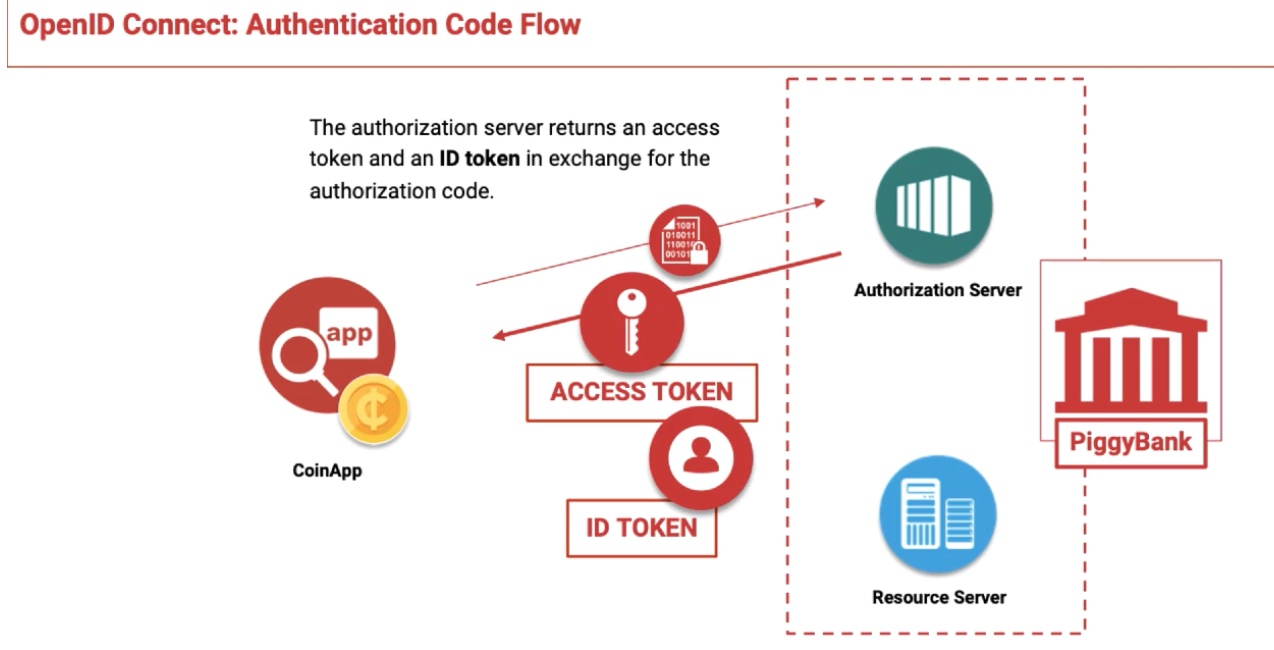
Claims used by Open ID connect

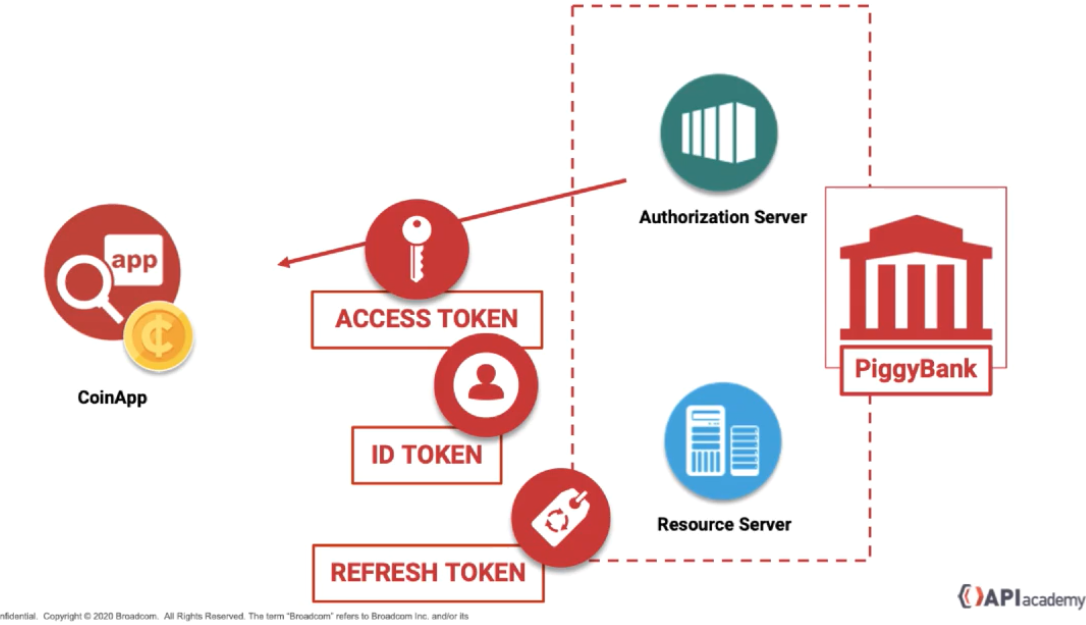


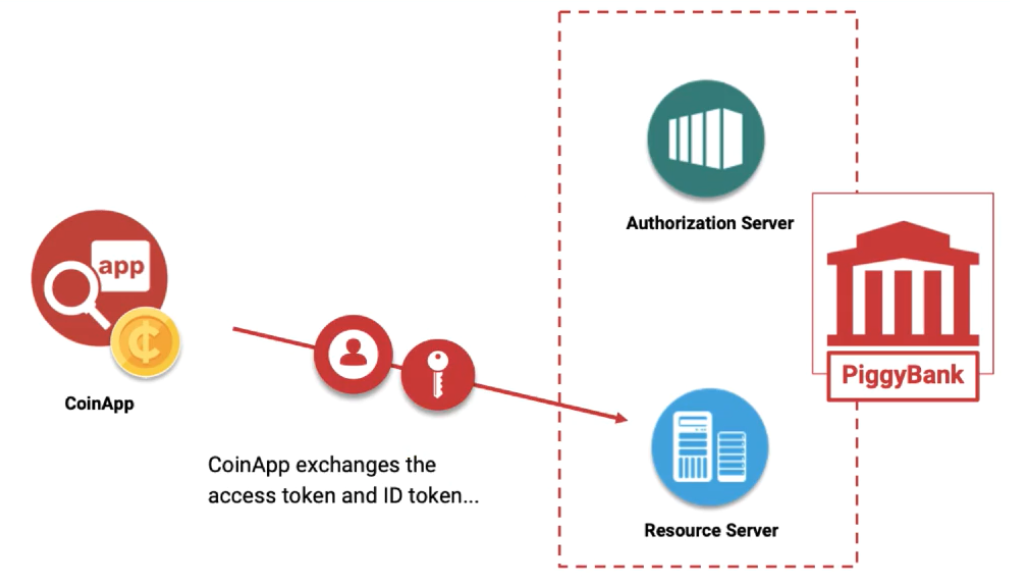
In our example we use only 3

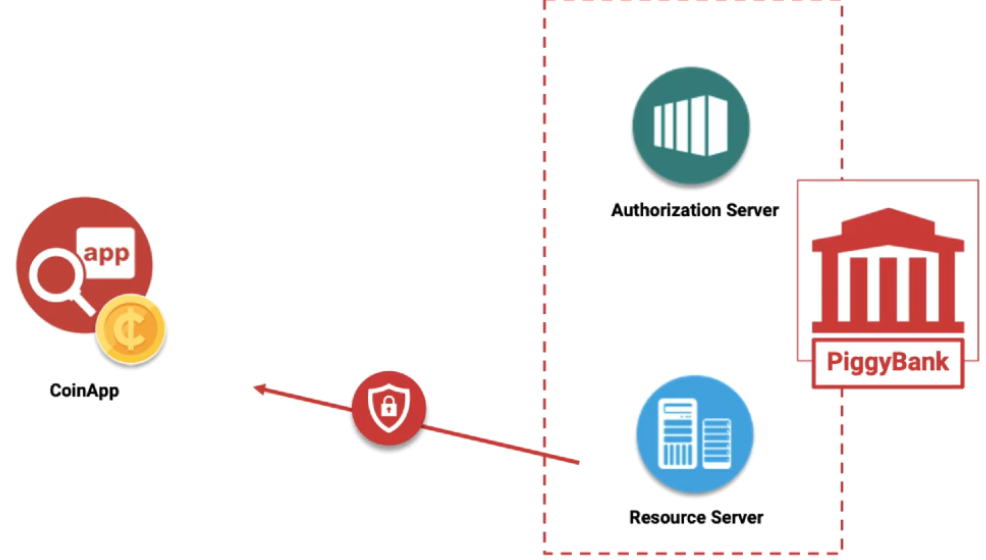


OPEN ID connect Authorization Code Flow



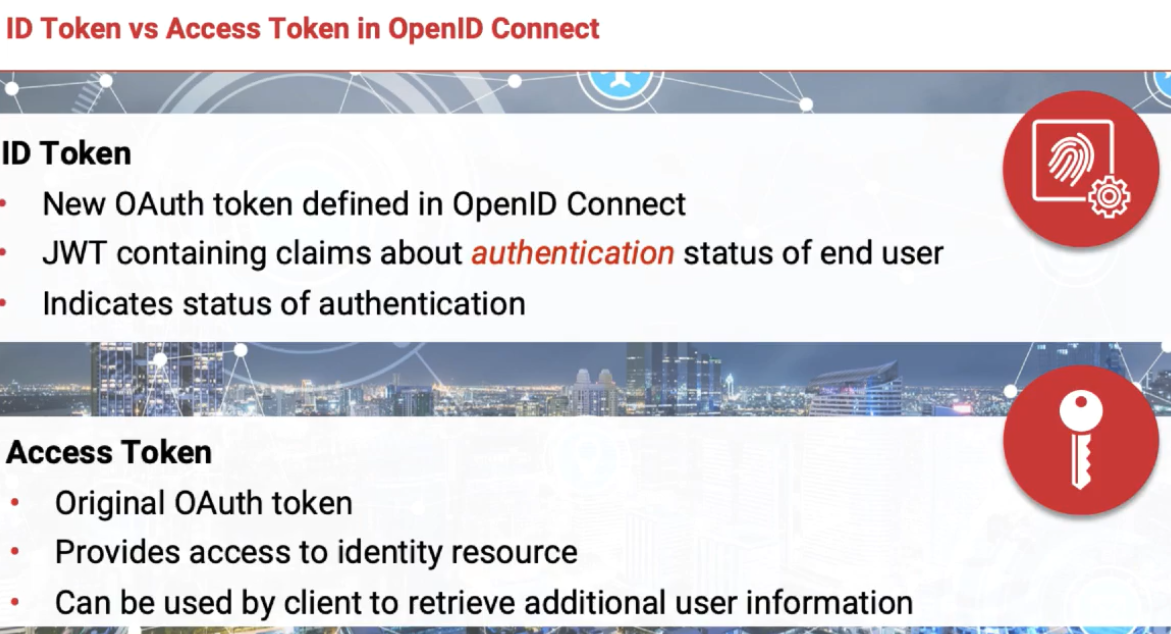






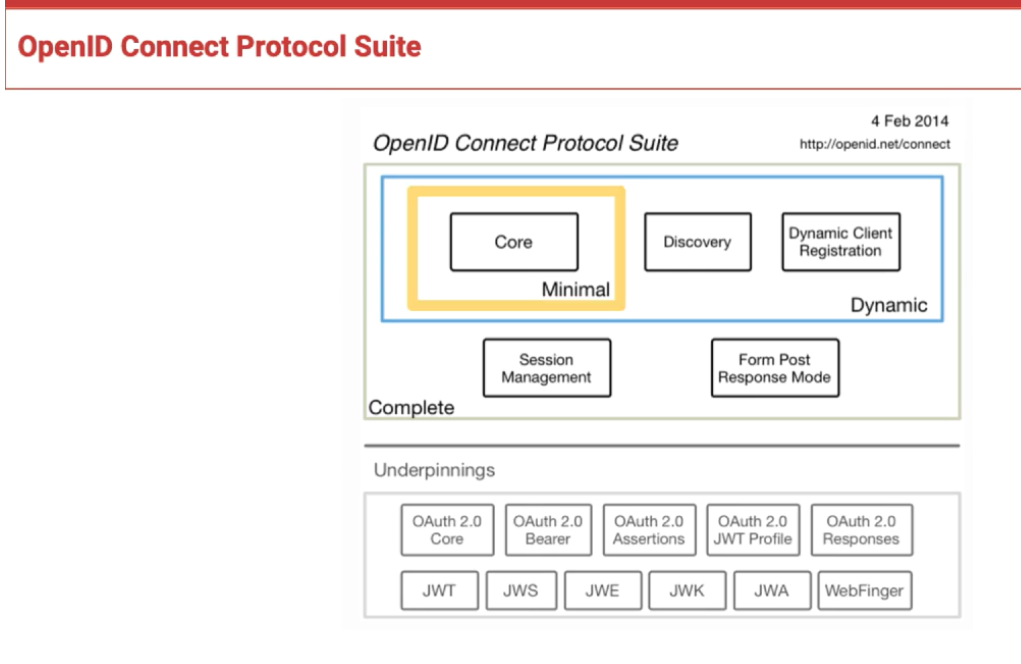


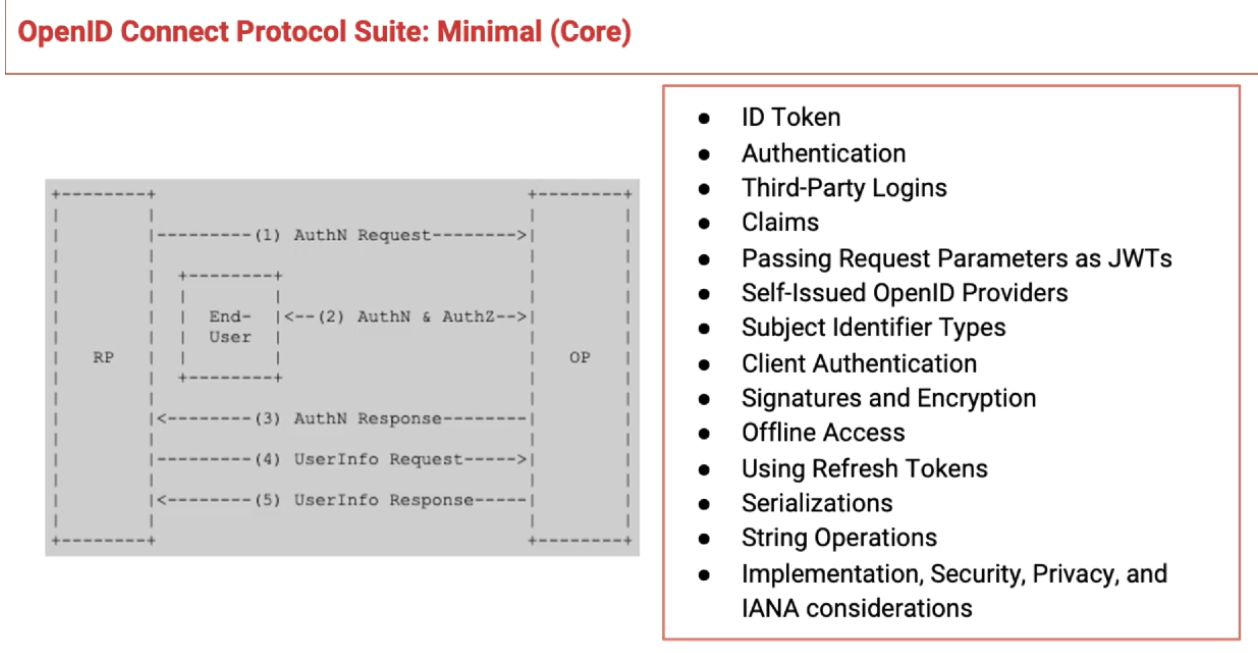
Userinfo endpoint



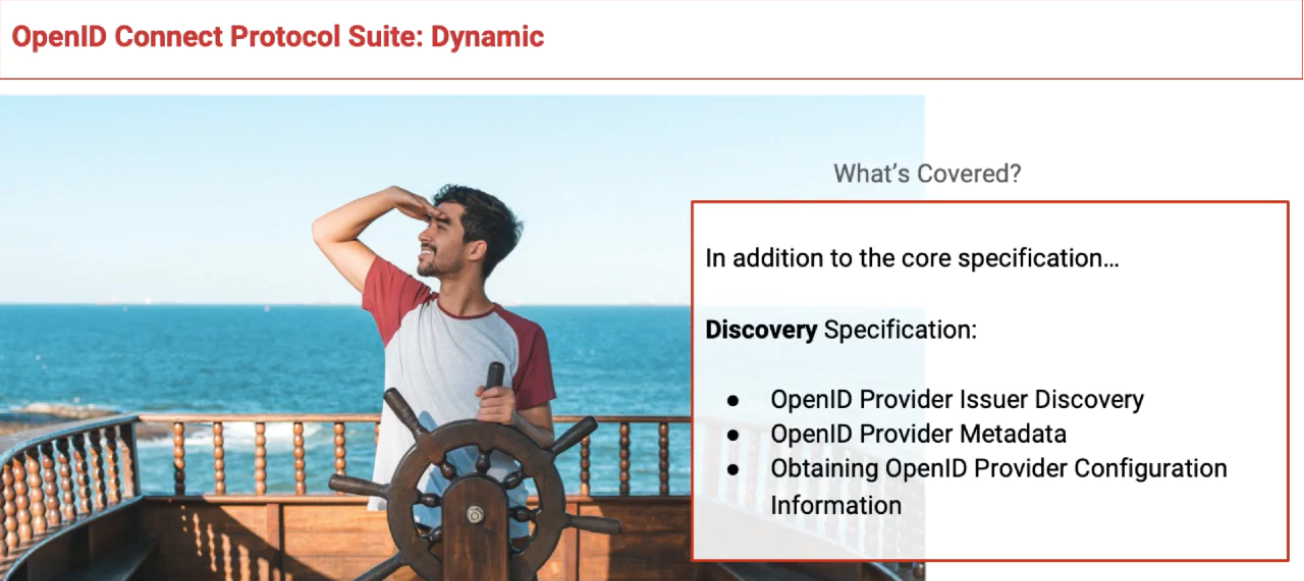
OPEN ID Connect suite can be implemented at 3 different levels.

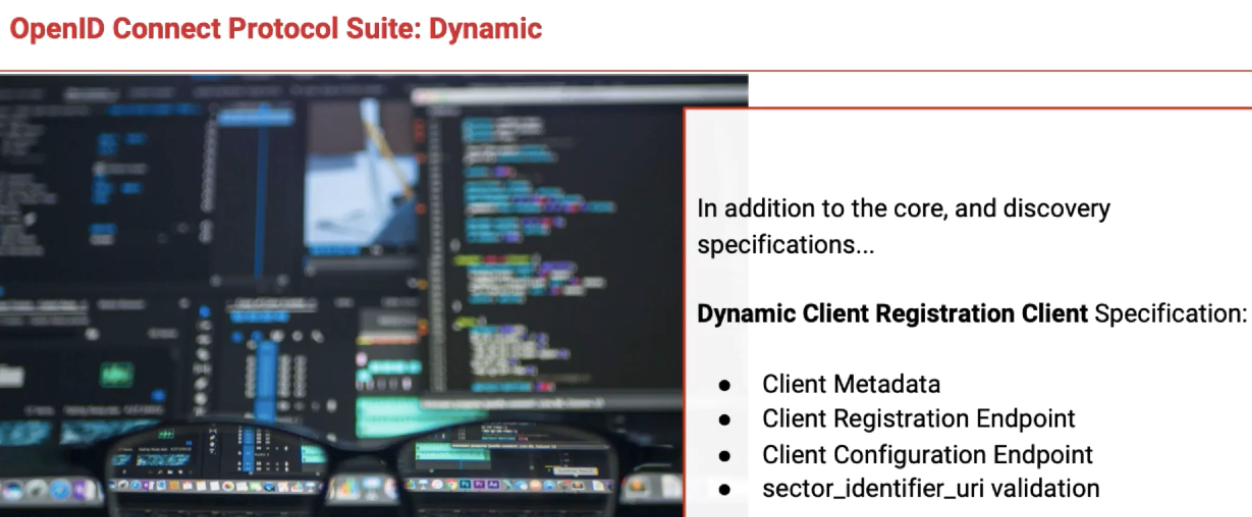
1. Minimal
2. Dynamic
3. Complete



Core components of minimal 

Dynamic = Core spec + Discovery spec list as below





Complete spec = Dynamic + Session Management specification

