* OpenID is an open standard and decentralized authentication protocol. Promoted by the non-profit OpenID Foundation, it allows users to be authenticated by co-operating sites (known as relying parties, or RP) using a third-party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log into multiple unrelated websites without having to have a separate identity and password for each.
* An end-user is the entity that wants to assert a particular identity. A relying party (RP) is a web site or application that wants to verify the end-user's identifier. Other terms for this party include "service provider" or the now obsolete "consumer". An identity provider, or OpenID provider (OP) is a service that specializes in registering OpenID URLs or XRIs. OpenID enables an end-user to communicate with a relying party. This communication is done through the exchange of an identifier or OpenID, which is the URL or XRI chosen by the end-user to name the end-user's identity.
* **PKCE** (RFC 7636: Proof Key for Code Exchange)

tools.ietf.org/html/rfc7636

PKCE (RFC 7636) is an extension to the Authorization Code flow to prevent certain attacks and to be able to securely perform the OAuth exchange from public clients.

* Difference Between OAUTH, OpenID and OPENID Connect in very simple term?

<https://security.stackexchange.com/questions/44611/difference-between-oauth-openid-and-openid-connect-in-very-simple-term>

* <https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc>
* <https://www.pingidentity.com/en/company/blog/posts/2018/securely-using-oidc-authorization-code-flow-public-client-single-page-apps.html>
* <https://auth0.com/docs/quickstart/webapp/aspnet-core/01-login>