What is a self-signed root CA?
A CA that does not rely on another CA for its validation is called a “root” (or “anchor”) CA. A CA that does rely on another CA for its validation is called an “intermediate CA”. Trust in such a root CA must be established by means other than a certificate. Your computer’s system software contains a list of acceptable root CA identities that have been pre-qualified by Apple. You can add other CAs to this list using the Keychain Access application, or your administrator can do this for you.

What is an intermediate certificate authority?
A certificate authority (CA) that relies on another CA for its validation is called an Intermediate CA. An intermediate CA depends on the CA that issued it for its validity, and can be invalidated, or revoked, by it. Intermediate CAs are commonly used by their issuing CA to delegate authority for a subset of its operation, such as a particular usage or class of users. If you or your system trusts an intermediate CA’s issuer, it will also trust the intermediate CA, unless you explicitly override this. You can also directly assign trust to an intermediate CA without trusting its issuer; however, this circumvents validity checks based on the issuer’s authority. When creating an intermediate CA with the Certificate Assistant, an existing root or intermediate CA (along with their corresponding private key) must be present to sign it.

What does “Make this CA the default” mean?
When accepting certificate signing requests from users, the default CA will be automatically selected in the popup menu of available Certificate Authorities. When you click “Make this CA the default”, the CA name you have specified above will become the default CA.