

sci.crypt: Re: How can I act as a Certificate Authority (CA) with openssl ??

## Re: How can I act as a Certificate Authority (CA) with openssl ??

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1088.html>

---

*From:* Joachim Ring ([jring\\_at\\_web.de](mailto:jring_at_web.de))

*Date:* 09/30/04

Date: 29 Sep 2004 16:04:20 -0700

- > *but there is no mention of what processes the CA will use to sign it –*
- > *there is mention of the file ca.txt, but that does not seem to exist.*
- > *I assume the CA will need to generate public and private keys for*
- > *themselves, then sign your certificate (cert.scr in the above*
- > *example), but what is the exact process? Can anyone give me some*
- > *openssl commands that will do it?*
- >
- > *I want to create certificates for Apache 2.x.*

try [http://www.modssl.org/docs/2.8/ssl\\_faq.html#ToC29](http://www.modssl.org/docs/2.8/ssl_faq.html#ToC29)

the process is the same for apache2 or in fact anything that uses x509 certificates in PEM format.

if you want to delve into the depths of it you might want to have a closer look at the docs for openssl ca module under

<http://www.openssl.org/docs/apps/ca.html#>

the general process to set up a ca is to generate key pair, generate self-signed ca certificate, store private key in a very safe place, distribute ca certificate to anybody to trust your ca (ideally by convincing browser manufacturers to put it into their products by default), sign certificate requests and keep good track of all certs issued.

if a cert needs to be revoked, a new revocation list should be published on the locations which should be mentioned under CRL distribution points in the ca cert asap.

joachim