

## Re: guidance on SSL certs and Apache2

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Debian/2005-09/2382.html>

---

**From:** Roberto C. Sanchez (*roberto\_at\_familiasanchez.net*)

**Date:** 09/19/05

Date: Mon, 19 Sep 2005 07:05:23 -0400

To: debian-user@lists.debian.org

On Sun, Sep 18, 2005 at 10:05:26PM -0700, Ross Boylan wrote:

> *I'm trying to set up apache2 to use ssl. I see numerous bugs about*  
> *this, including the fact that the setup is neither automated nor documented*  
> *(267477 -- which includes some recipes and references to help) and*  
> *that a tool, ssl-cert, used at one point by apache2 for debconf, has*  
> *problems (230485). The changelog says that ssl-cert was dropped for*  
> *the setup.*

>

> *There seem to be at least 3 ways to setup certificates:*

> *openssl*

> *ssl-cert*

> *apache2-ssl-certificate*

>

> *There is a configuration file /etc/ssl/openssl.cnf, and there seems to*

> *be space for certificates and keys under /etc/ssl/ and*

> */etc/apache2/ssl.*

>

> *Can anyone suggest which of these knobs I should tweak to set things*

> *up? And where should I put the resulting files? I use KDE, and I see*

> *it has Kleopatra for certificate management. Is that useable?*

>

> *I want to be my own CA as well as having the certificates (one for*

> *each virtual domain).*

>

OK. Here are my notes:

New Certificate Authority:

Check out the SSL HOWTO.

New Certificate:

(All actions take place inside of /etc/ssl)

```
vi openssl.cnf (change default days if desired)
```

```
for i in `ls -1 *.pem` ; do mv $i $i.old-$(date +%Y%m%d); done
```

## Debian–User: Re: guidance on SSL certs and Apache2

```
openssl req -new -key server.key -out newreq.pem
vi openssl.cnf (change default days back to normal)
openssl ca -revoke demoCA/newcerts/<num of previous cert>.pem
openssl ca -gencrl -out demoCA/crl/sopac-ca.crl
cp demoCA/crl/sopac-ca.crl /var/www/ca.crl
openssl ca -policy policy_anything -out newcert.pem -infile newreq.pem
cat newcert.pem | sed -n '/BEGIN/,/END/p' >server.pem
cat server.key >> server_key_and_cert.pem
cat server.pem >> server_key_and_cert.pem
chmod -R o-rx *
# chgrp mail server_key_and_cert.pem # T
```