

## Contents

1	How to setup SSL on courier-imap working under qmail	1
2	The steps required	1
3	Create a Certificate Authority (CA)	2
4	Create a certificate request for courier-imap	3
5	Sign this certificate by your CA	4
6	Create the .pem file for courier-imap and configure courier-imap	5
7	Adding the Diffie-Hellman Block to the .pem file	5
8	Configure courier-imap	5
9	Install the root certificate of your CA in Netscape/Mozilla or Internet Explorer	6
10	Make your Emailclient connect with SSL	6
11	All in One Script	6

## 1 How to setup SSL on courier-imap working under qmail

Reading Email over an untrusted Net (i.e. almost every Net), usually comprises a big lack on security. Namely your login and password will be sent in plaintext to the mailserver. In times where sniffing is a question of launching a little tool (ettercap, dsniff a.o.), login in to pop or imap servers requires an encryption in order to avoid a sniffer to read your emails (and maybe even login to a hole computer system). courier-imap comes with the ability to make a SSL (Secure Socket Layer) connection to your emailclient over the Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP).

## 2 The steps required

To make courier-imap run with SSL (we assume you have installed courier-imap and openssl), you have to do the following steps:

- §3
- §4

- §5
- §??
- §7
- §8 =item \*  
§9
- §10

### 3 Create a Certificate Authority (CA)

Create a directory where you store your certificates and keys. For example

```
# mkdir /root/myCA
# cd /root/myCA
```

Type in your console

```
# openssl genrsa -des3 -out ca.key 2048
```

to generate a 2048 Bit RSA key pair. You will see something like this:

```
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Enter a Password twice. After executing this, you will have the 2048 Bit key stored in ca.key. Now ou have to create a self signed CA-certificate:

```
# openssl req -new -x509 -days 3652 -key ca.key -out ca.crt
```

You will see something like

```
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CH
State or Province Name (full name) [Some-State]:Zuerich
```

```
Locality Name (eg, city) []:.  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Make a Cert Inc.  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:mail.mydomain.com  
Email Address []:myname@mydomain.com
```

Firs give the password specified in the first step and then fill out all wished values. Now we have created a CA certificate called ca.crt, valid for 10 years.

## 4 Create a certificate request for courier-imap

Now we almost do the same as in the first step. First we create a key pair, then we make a certificate request wich we then sign by the CA. Ok, let's make a new 2048 Bit key:

```
# openssl genrsa -out pop3d.key 2048
```

This time we will not be asked to define a password:

```
Generating RSA private key, 2048 bit long modulus  
.....+++  
.....+++  
e is 65537 (0x10001)
```

The next step is to make a certificate request. Type

```
# openssl req -new -key pop3d.key -out pop3d.csr
```

The Output looks like

```
Using configuration from /usr/share/ssl/openssl.cnf  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:CH  
State or Province Name (full name) [Some-State]:Zuerich  
Locality Name (eg, city) []:Zuerich  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My very personal IMAP/POP Ser  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:pop3.mydomain.com  
Email Address []:postmaster@mydomain.com
```

Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:

Important is the point **Common Name**, where you have to specify exactly  
the same name, as your server has. E.g. type *pop3.mydomain.com* if you want  
to access your mailserver with this URL. Leave the optional password blank.

## 5 Sign this certificate by your CA

The easiest way to sign the certificate of your mailserver (the one called *pop3.mydomain.com*),  
is the use of the script 'sign.sh', which comes with the `mod_ssl` package. If you  
don't find it, you can download it a href=""/>

Type

```
# ./sign.sh pop3d.csr
```

(maybe you have to give the full path to the sign script). It will output  
something like

```
CA signing: pop3d.csr -> pop3d.crt:
Using configuration from ca.config
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName :PRINTABLE:'CH'
stateOrProvinceName :PRINTABLE:'Zuerich'
localityName :PRINTABLE:'Zuerich'
organizationName :PRINTABLE:'My very personal IMAP/POP Server Inc.'
organizationalUnitName:PRINTABLE:''
commonName :PRINTABLE:'pop3.mydomain.com'
emailAddress :IA5STRING:'postmaster@mydomain.com'
Certificate is to be certified until Jan 19 21:42:14 2003 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
CA verifying: pop3d.crt <-> CA cert
pop3d.crt: OK
```

Now we have our signed Certificate for the imap/pop server called *pop3d.crt*.

## 6 Create the .pem file for courier-imap and configure courier-imap

What we finally need to do, is create the .pem file, which courier-imap can read. Edit the pop3d.crt file and delete all lines except those between the lines

```
-----BEGIN CERTIFICATE-----  
  
and  
  
-----END CERTIFICATE-----
```

After that we have to concatenate the content of pop3d.crt and pop3d.key in a new file called **pop3d.pem**:

```
# cat pop3d.key pop3d.crt > pop3d.pem
```

## 7 Adding the Diffie-Hellman Block to the .pem file

Type

```
# openssl gendh >> pop3d.pem  
  
to add the Diffie-Hellman Code Block to pop3d.pem.  
The output looks like
```

```
Generating DH parameters, 512 bit long safe prime, generator 2  
This is going to take a long time  
.....+.....+*****+*****
```

## 8 Configure courier-imap

First you have to copy the .pem file to the imap server's directory. In case of a standard courier-imap installation you may do this with

```
# cp pop3d.pem /usr/lib/courier-imap/share/  
  
and  
  
# chmod 0600 /usr/lib/courier-imap/share/pop3d.pem
```

Otherwise locate your courier-imap directory. The second step is very important! Then edit the **imapd-ssl** Configfile of courier-imap, which usually resides in /usr/lib/courier-imap

```
# vim /usr/lib/courier-imap/etc/imapd-ssl
```

and change the line

```
IMAPDSSLSTART=NO
```

to

```
IMAPDSSLSTART=YES
```

After that you have to restart courier-imap.

## 9 Install the root certificate of your CA in Netscape/Mozilla or Internet Explorer

If you like, you can place a copy of your ca.crt file to a location where your webserver (if any) has access, in order that people using your pop/imap server can easily install the CA certificate. See the [securemailer.ch](http://securemailer.ch) homepage for a sample. Clicking on the ca.crt link will open in Netscape/Mozilla and Internet Explorer a window, which lets you install the certificate.

## 10 Make your Emailclient connect with SSL

Last but not least you may configure your Emailclient in order to connect with SSL to your pop/imap server. In Netscape/Mozilla click the *'Edit'* Menu and then on *'Mail and Newsgroups Account Settings'*, then on the Mailaccount of your choice and on *'Server Settings'* where you find the Checkbox *Use Secure Connection (SSL)*. For IE Help read one of the well documented Helps inside IE.

## 11 All in One Script

I wrote a perl Script which makes all those steps in one. Just download the `it|ca/make_courier_cert.pl` entry elsewhere in this document and run it:

```
# ./make_courier_cert.pl
```

Fill out all values as described in this document and you'll have a wonderful `pop3.pem` file copied directly in your courier-imap share directory. Just make sure, you have the `sign.sh` script in the same directory as the *'All in One'* Script.

### Author

Rafael Perez, [securemailer at superrafi dot com](mailto:securemailer@superrafi.com)