

Sendmail: TLS handshake failed

if you find TLS handshake errors in your sendmail like this:

```
May 10 15:36:17 mail sm-mta[28953]: u4A8Maoa020509: to=<***@domain.it>, ctladdr=<***@domain.com> (1501/2000), delay=05:13:39, xdelay=00:00:00, mailer=esmtplib, pri=1051530, relay=aserver.domain.it. [xxx.xxx.xxx.xxx], dsn=4.0.0, stat=Deferred: 403 4.7.0 TLS handshake failed.
```

check the configs, if defined:

`_my_hostname.mc`

```
define(`CERT_DIR', `/etc/mail/certs')dnl
define(`confDH_PARAMETERS', `CERT_DIR/dh.param')dnl
```

suppose your `CERT_DIR` is `"/etc/mail/certs"`:

```
cd /etc/mail/certs
openssl dhparam -out dh.param 2048
cd /etc/mail && make stop && make start
```

We can use a key len of 4096 too, but it is longer to generate and adds a lot of complexity. So for me 2048 it good enough.

—
return to gimbo wiki [home page](#)

From:
<https://wiki.gimbo.org/> - **wiki.gimbo.org**

Permanent link:
https://wiki.gimbo.org/doku.php?id=public:sendmail_tls_error

Last update: **13.03.2022 05:55**

