

SSL сертификат для Postfix

Create a root private key:

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

Change permissions of this private key to 400:

```
# chmod 400 /usr/share/ssl/certs/postfix/rootCA.key
```

Create self-signed root certificate:

```
# openssl req -x509 -new -nodes -key rootCA.key -days 1024 -  
out rootCA.pem
```

With the following data (change information to required):

```
Country Name (2 letter code) [AU]:XX  
State or Province Name (full name) [Some-State]:SomeState  
Locality Name (eg, city) []:SomeCity  
Organization Name (eg, company) [Internet Widgits Pty  
Ltd]:Company Co  
Organizational Unit Name (eg, section) []:Company Co  
Common Name (e.g. server FQDN or YOUR name) []:example.com  
Email Address []:admin@example.com
```

Create private key for final certificate:

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

Create certificate sign request:

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

And finally create server certificate based on root CA certificate and root private key:

```
# openssl x509 -req -in device.csr -CA rootCA.pem -CAkey  
rootCA.key -CAcreateserial -out device.crt -days 500
```

Change Postfix configuration /etc/postfix/main.cf to use the newly created certificates:

```
#smtpd_tls_key_file = /etc/postfix/postfix_default.pem
```

```
#smtpd_tls_cert_file = /etc/postfix/postfix_default.pem
#smtpd_tls_CAfile = /etc/postfix/postfix_default.pem
smtpd_tls_key_file = /usr/share/ssl/certs/postfix/device.key
smtpd_tls_cert_file = /usr/share/ssl/certs/postfix/device.crt
smtpd_tls_CAfile = /usr/share/ssl/certs/postfix/rootCA.pem
```

Restart postfix service:

```
[root@centos ~]# service postfix restart
Shutting down postfix: [
OK ]
Starting postfix: [
OK ]
```

All newly generated files should be created in folder /usr/share/ssl/certs/postfix/ (you could change folder, but paths in Postfix configuration have to be changed too).

After these steps, Postfix will work with the new certificates:

```
[root@centos ~]# openssl s_client -crlf -connect localhost:465
CONNECTED(00000003)
depth=0 C = US, ST = SomeState, L = SomeCity, O = Company Co,
OU = Company Co, CN = example.com, emailAddress =
admin@example.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = SomeState, L = SomeCity, O = Company Co,
OU = Company Co, CN = example.com, emailAddress =
admin@example.com
verify return:1
---
Certificate chain
 0 s:/C=PK/ST=SomeState/L=SomeCity/O=Company Co/OU=Company
Co/CN=example.com/emailAddress=admin@example.com
  i:/C=PK/ST=SomeState/L=SomeCity/O=Company Co/OU=Company
Co/CN=example.com/emailAddress=admin@example.com
---
```

<https://support.plesk.com/hc/en-us/articles/213402809-How-to-generate-custom-self-signed-SSL-certificates-and-apply-it-to->

Postfix