Pełny certyfikat SSL - apache

Uruchomienie modułu ssl

```
fatrg@LAPTOP-3OASB45S:/etc/apache2$ sudo a2enmod ssl
[sudo] password for fatrg:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
```

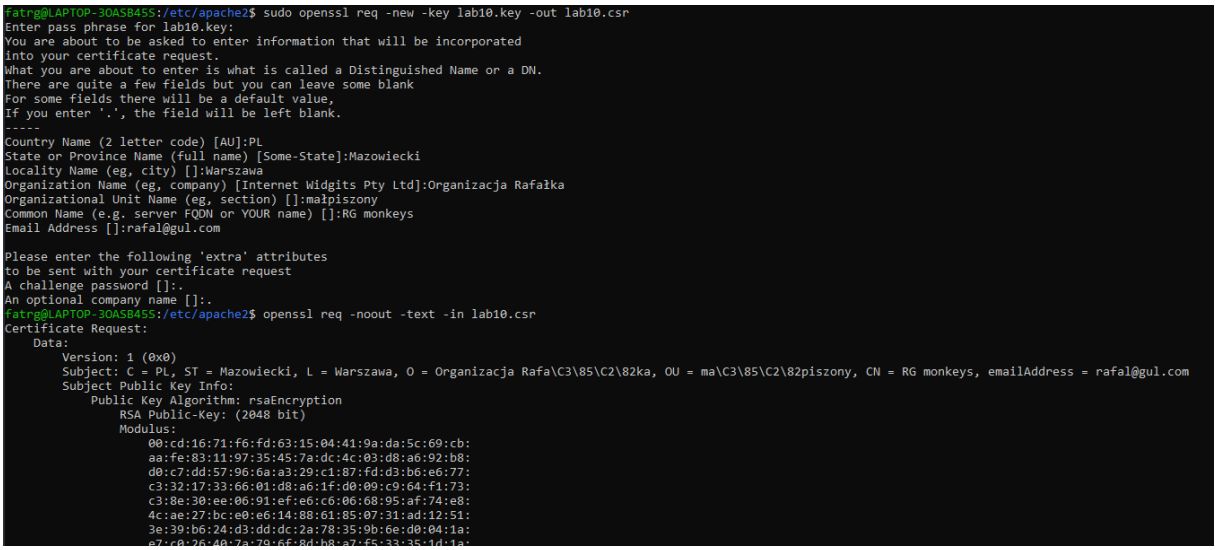
Utworzenie klucza

```
fatrg@LAPTOP-3OASB45S:/etc/apache2$ sudo openssl genrsa -aes256 -out lab10.key
Generating RSA private key, 2048 bit long modulus
.....................................................................................................+++++
.........................+++++
e is 65537 (0x010001)
Enter pass phrase for lab10.key:
Verifying - Enter pass phrase for lab10.key:
fatrg@LAPTOP-3OASB45S:/etc/apache2$ ls -al
total 48
drwxr-xr-x 1 root root   512 Dec 13 01:10 .
drwxr-xr-x 1 root root   512 Dec 13 00:32 ..
-rw-r--r-- 1 root root  7259 Nov 22 22:28 apache2.conf
drwxr-xr-x 1 root root   512 Nov 22 22:13 conf-available
drwxr-xr-x 1 root root   512 Nov 22 22:13 conf-enabled
-rw-r--r-- 1 root root  1782 Nov 22 21:42 envvars
-rw------- 1 root root  1766 Dec 13 01:11 lab10.key
```

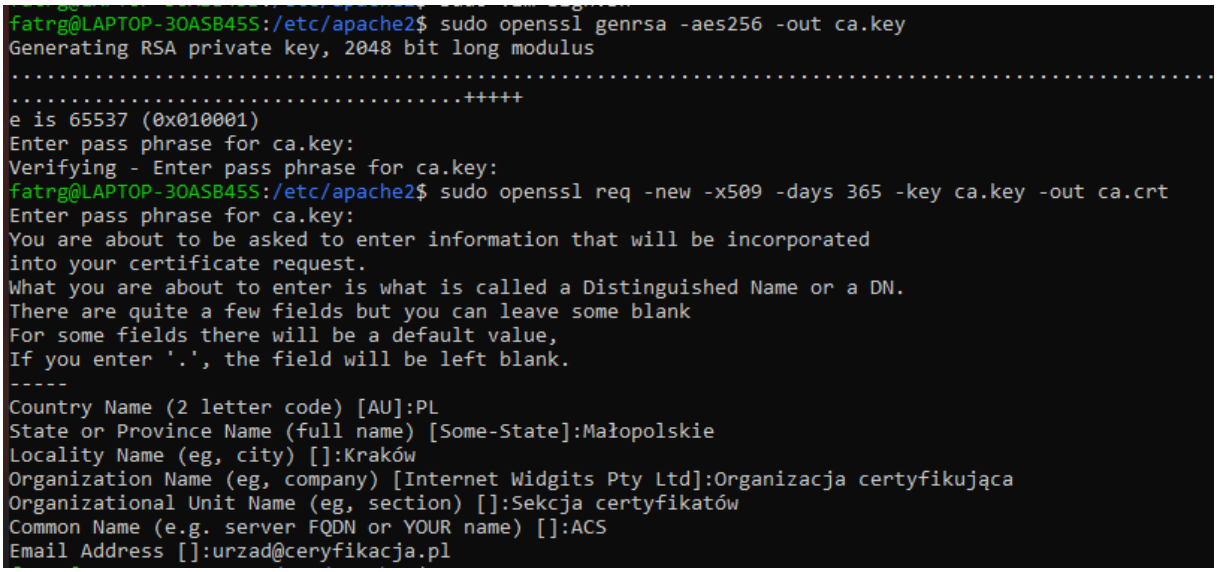
Sprawdzenie utworzonego klucza

```
fatrg@LAPTOP-3OASB45S:/etc/apache2$ sudo openssl rsa -noout -text -in lab10.key
Enter pass phrase for lab10.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:cd:16:71:f6:fd:63:15:04:41:9a:da:5c:69:cb:
    aa:fe:83:11:97:35:45:7a:dc:4c:03:d8:a6:92:b8:
    d0:c7:dd:57:96:6a:a3:29:c1:87:fd:d3:b6:e6:77:
    c3:32:17:33:66:01:d8:a6:1f:d0:09:c9:64:f1:73:
    c3:8e:30:ee:06:91:ef:e6:c6:06:68:95:af:74:e8:
```

Wysłanie prośby o autoryzację



Utworzenie „urzędu certyfikującego”



Podpisanie certyfikatu

```
fatrg@LAPTOP-3OASB45S:/etc/apache2$ sudo ./sign.sh lab10.csr
CA signing: lab10.csr -> lab10.crt:
Using configuration from ca.config
Enter pass phrase for /etc/apache2/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'PL'
stateOrProvinceName   :ASN.1 12:'Mazowiecki'
localityName          :ASN.1 12:'Warszawa'
organizationName      :ASN.1 12:'Organizacja Rafa\0xFFFFFFC3\0xFFFFFF85\0xFFFFFFC2\0xFFFFFF82ka'
organizationalUnitName:ASN.1 12:'ma\0xFFFFFFC3\0xFFFFFF85\0xFFFFFFC2\0xFFFFFF82piszony'
commonName            :ASN.1 12:'RG monkeys'
emailAddress          :IA5STRING:'rafal@gul.com'
Certificate is to be certified until Dec 13 01:27:03 2022 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: lab10.crt <-> CA cert
lab10.crt: OK
```

Certyfikat na stronie https://localhost:4443/