

Sprawozdanie

LABORATORIUM 6. INFRASTRUKTURA KLUCZA PUBLICZNEGO, PODPIS CYFROWY, SSL/TLS

Zadanie 6.6. Utworzenie podpisu cyfrowego

```
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl genrsa -aes256 -out private.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.key:
Verifying - Enter pass phrase for private.key:
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl rsa -in private.key -out public.pem -outform PEM -pubout
Enter pass phrase for private.key:
writing RSA key
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl dgst -sha256 -sign private.key -out podpis.sha256 podpis.txt
Enter pass phrase for private.key:
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt
Verified OK
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt
Verification Failure
student@Kubuntu:~/Documents/lab10/zad 6.6$ openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt
Verified OK
```

P.6.7. Udokumentuj poprawność przeprowadzonego ćwiczenia i opisz uzyskane wyniki. Omów jak wpływa modyfikacja wiadomości na weryfikację podpisu cyfrowego.

Wygenerowaliśmy klucz prywatny oraz publiczny. Podpisaliśmy plik z wykorzystaniem klucza prywatnego. Weryfikacja zachodzi w sposób poprawny. Po zmianie treści pliku weryfikacja daje wynik negatywny. Po naprawieniu pliku do stanu początkowego weryfikacja się udaje.

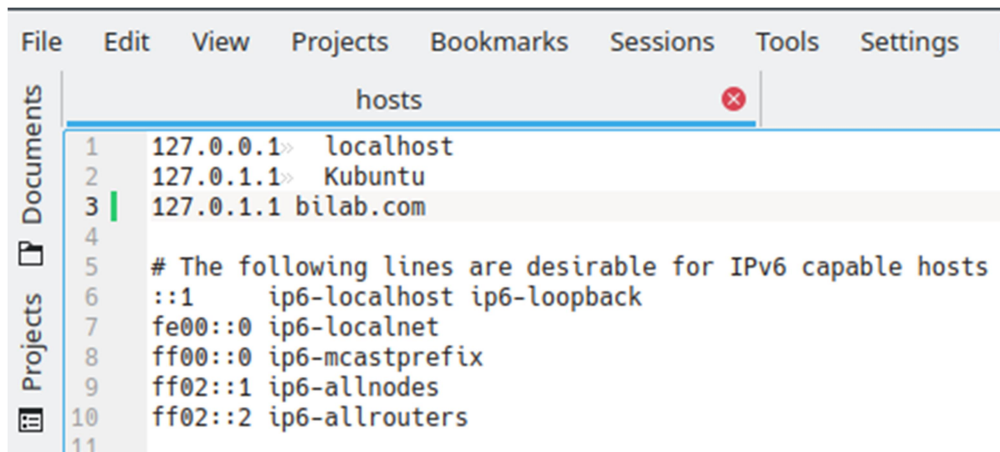
Zadanie 6.7. Konfiguracja HTTPS na serwerze Apache

D.5.2. Jakie kroki należy podjąć żeby uzyskać połączenie? Udokumentuj poprawność konfiguracji i komunikacji klient-serwer. Omów uzyskane efekty.

Generujemy i podpisujemy parę kluczy i certyfikat dla serwera.

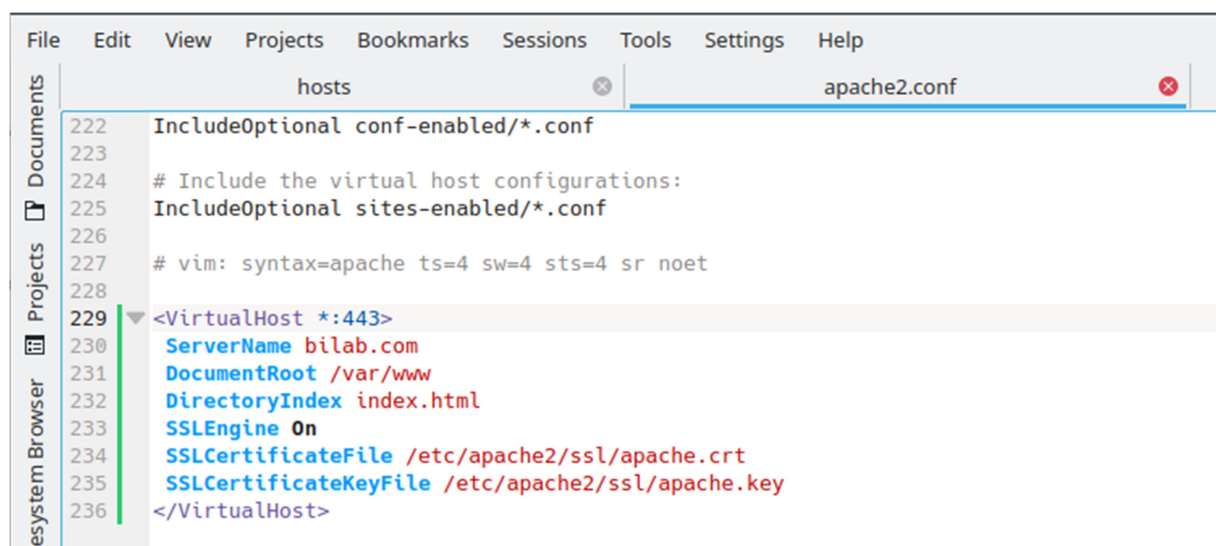
```
student@Kubuntu:~/Documents/lab10/zad 6.7$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about 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]:PL
State or Province Name (full name) [Some-State]:LUB
Locality Name (eg, city) []:LUBLIN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:POLLUB
Organizational Unit Name (eg, section) []:BI
Common Name (e.g. server FQDN or YOUR name) []:bilab.com
Email Address []:bilab@bilab.pl
```

Dodajemy domenę:



```
File Edit View Projects Bookmarks Sessions Tools Settings
hosts
1 127.0.0.1> localhost
2 127.0.1.1> Kubuntu
3 127.0.1.1 bilab.com
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1 ip6-localhost ip6-loopback
7 fe00::0 ip6-localnet
8 ff00::0 ip6-mcastprefix
9 ff02::1 ip6-allnodes
10 ff02::2 ip6-allrouters
11
```

Konfigurujemy serwer do pracy z HTTPS



```
File Edit View Projects Bookmarks Sessions Tools Settings Help
hosts apache2.conf
222 IncludeOptional conf-enabled/*.conf
223
224 # Include the virtual host configurations:
225 IncludeOptional sites-enabled/*.conf
226
227 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
228
229 <VirtualHost *:443>
230     ServerName bilab.com
231     DocumentRoot /var/www
232     DirectoryIndex index.html
233     SSLEngine On
234     SSLCertificateFile /etc/apache2/ssl/apache.crt
235     SSLCertificateKeyFile /etc/apache2/ssl/apache.key
236 </VirtualHost>
```

Dodajemy w przeglądarce certyfikat urzędu certyfikacji:

