Laboratorium 8

Pobierz plik `lab8.tar.gz` i rozpakuj go. Plik zawiera przykłady serwera i klienta korzystającego z SSL w dwóch wersjach.
Zapoznaj się z krótkim wprowadzeniem do korzystania z OpenSSL.

Część 1: SSL

1. Przygotuj certyfikaty zgodnie z podaną poniżej procedurą:

Utwórz własny CA (Certificate Authority)

a) Utwórz klucz poziomu głównego i żądanie certyfikatu głównego (root level):

```
$ openssl req –newkey rsa:2048 –keyout root_key.pem –out root_request.pem
```

gdzie `root_key.pem` będzie zawierać klucz prywatny zaś `root_request.pem` żądanie certyfikatu.

b) Wygeneruj certyfikat główny:

```
$ openssl x509 –req –in root_request.pem –signkey root_key.pem \
  –out root_certificate.pem
```

gdzie `root_certificate.pem` będzie zawierać certyfikat.

c) Umieść certyfikat główny i klucz w jednym pliku:

```
$ cat root_certificate.pem root_key.pem > root.pem
```

d) Utwórz prywatny klucz CA i żądanie certyfikatu:

```
$ openssl req – newkey rsa:2048 –keyout CA_key.pem –out CA_request.pem
```

e) Utwórz certyfikat dla CA

```
$ openssl x509 –req –in CA_request.pem –CA root.pem –cAkey root.pem \
  –CAcreateserial –out CAcert.pem
```

f) Umieść certyfikat CA i klucz w jednym pliku:

```
$ cat CAcert.pem CA_key.pem  root_certificate.pem > CA.pem
```

Utwórz certyfikat serwera

a) Wygeneruj klucz prywatny (nieszyfrowany)

```
$ openssl genrsa 2048 > server_key.pem
```

b) Wygeneruj żądanie certyfikatu

```
$ openssl req –new –key server_key.pem –out server_request.pem
```

c) c) Utwórz certyfikat:

```
$ openssl x509 –req –in server_request.pem –CA Ca.pem –CAcreateserial \
  –Cakey CA.pem –out server_certificate.pem
```

d) Umieść certyfikat i klucz w jednym pliku:

```
$ cat server_ceryificate.pem server_key.pem CAcert.pem root_certificate.pem
> server.pem
```

2. Sprawdź działanie programów z pliku lab8.tar.gz.

3. Wzorując się na tych programach zmodyfikuj aplikację `serwerPliki` z laboratorium 3 tak, aby korzystała ona z SSL. Ustaw tak opcję gniazda `SO_REUSEADDR`, aby można było ponownie uruchamiać serwer na tym samym porcie, zaraz po jego zamknięciu.

4. Wzorując się na programach z pliku lab8.tar.gz zmodyfikuj wybrany serwer HTTP tak, aby korzystał on z SSL.