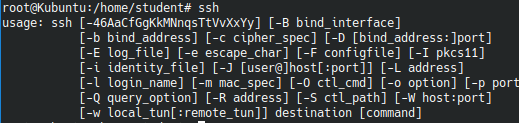
Sprawozdanie

# Zadanie 1. Należy w bezpieczny sposób umieścić przygotowaną stronę HTML we właściwym katalogu na serwerze Apache (maszyna serwer), Stronę należy przesłać z maszyny client wykorzystując protokół SSH i powiązane z nim narzędzia. W tym celu należy:

## zainstalować klienta SSH na maszynie client i serwer SSH na maszynie serwer,

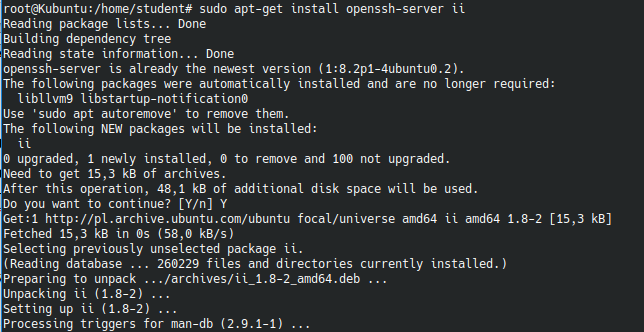
Klient SSH na urządzeniu będącym klientem jest już zainstalowany, możemy to sprawdzić za pomocą komendy:

ssh



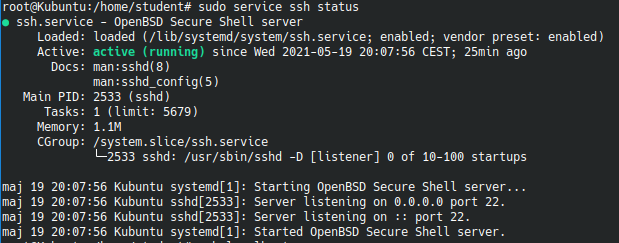
Na urządzeniu wirtualnym będącym serwerem instalujemy serwer SSH za pomocą komendy:

sudo apt-get install openssh-server ii



Następnie możemy sprawdzić działanie serwera za pomocą komendy:

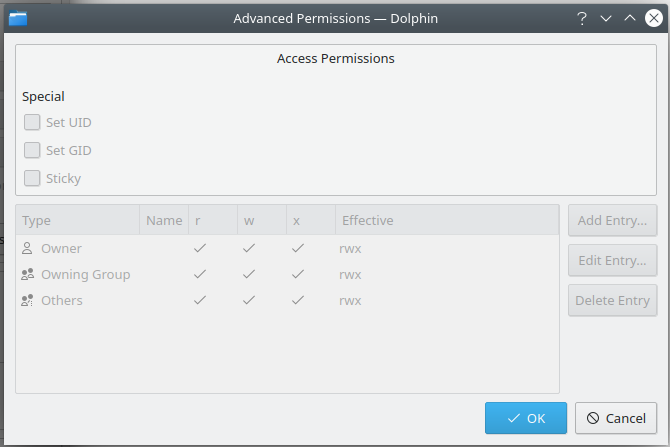
service ssh status



## utworzyć użytkownika na maszynie serwer oraz skonfigurować jego uprawnienia do korzystania z serwera Apache,

Po uprzednim wejściu w konsoli do katalogu /var/www nadajemy prawa do katalogu html komendą (nadałem uprawnienia wszystkim użytkownikom):

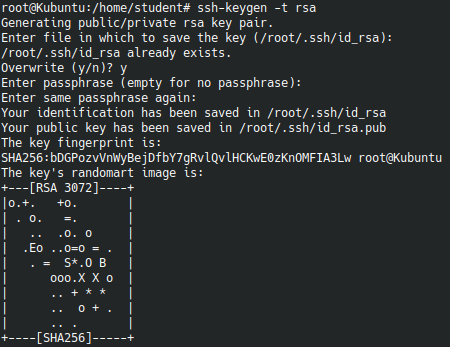
sudo chmod 777 html



## wygenerować klucze i dokonać ich dystrybucji tak by możliwe było logowanie na maszynie serwer bez konieczności podawania hasła.

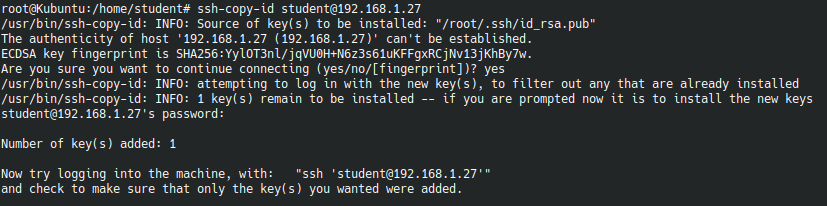
Tworzymy klucze komendą:

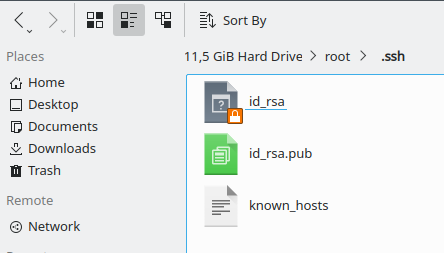
ssh-keygen -t rsa



Następnie przenosimy klucze komendą:

ssh-copy-id student@192.168.1.27

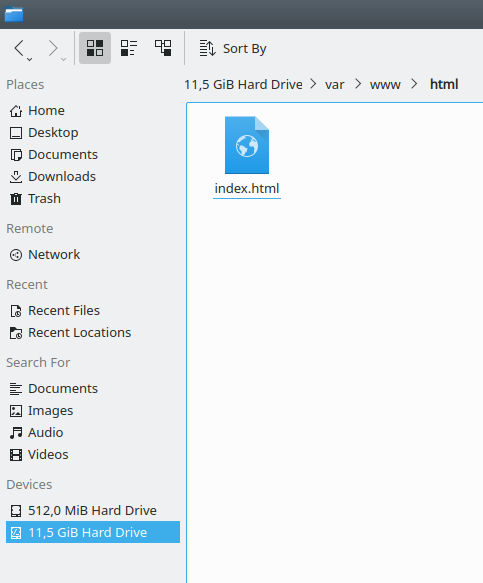




## przesłać przygotowaną stronę na serwer Apache z wykorzystanie połączenia szyfrowanego,

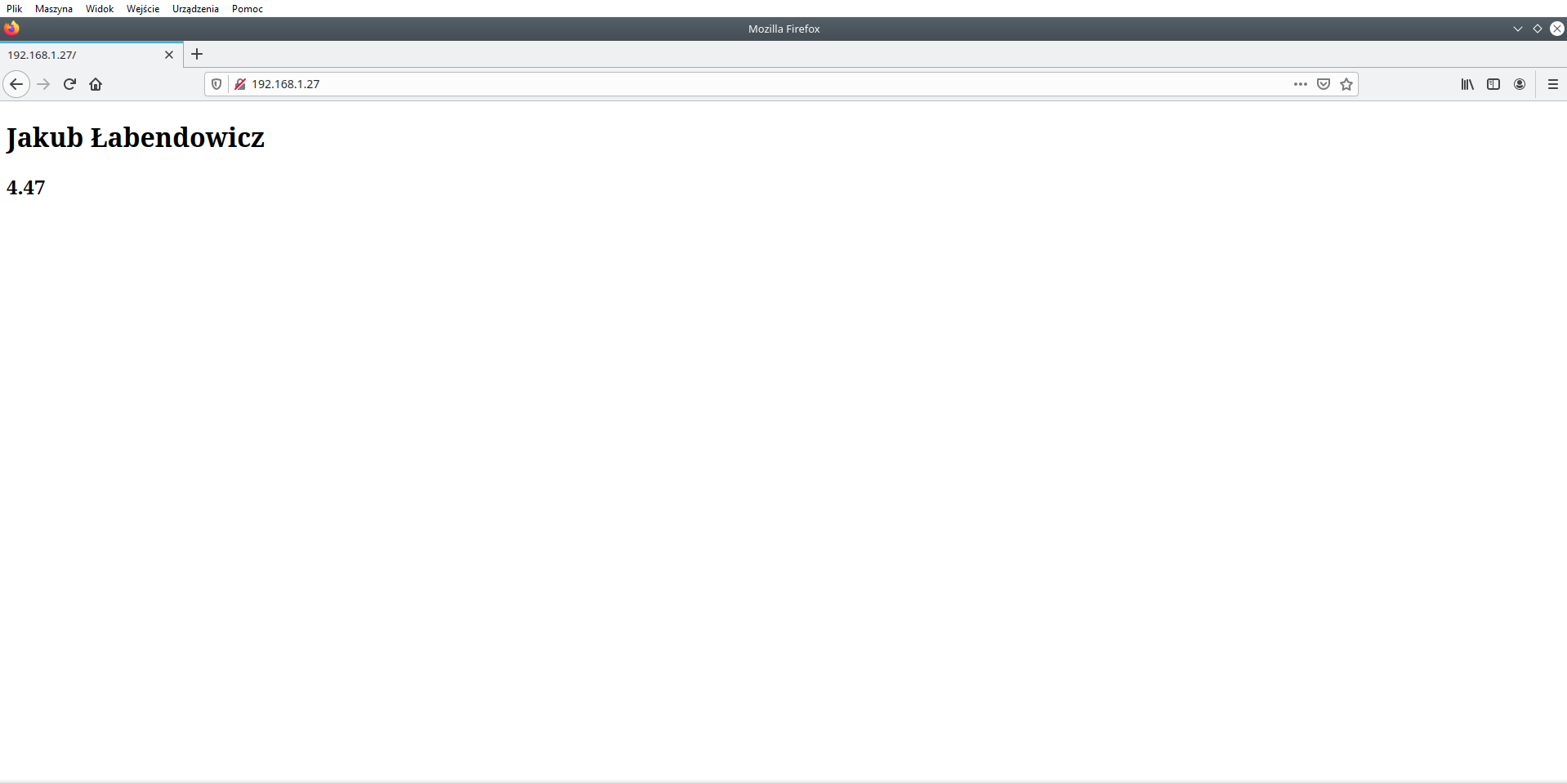
Przenosimy plik index.html z klienta na serwer komendą:

scp index.html [student@192.168.1.27:/var/www/html](mailto:student@192.168.1.27:/var/www/html)



## potwierdzić poprawność zrealizowanej konfiguracji przez zalogowanie się na serwerze Apache z przeglądarki działającej na maszynie client.

Otwieramy stronę z poziomu przeglądarki na maszynie będącej klientem:



# Zadanie 2. Należy, wykorzystując narzędzia z pakietu OpenSSL zainstalowanego na maszynie CA, należy utworzyć certyfikat dla serwera Apache w domenie zad1crypto.io . W tym celu należy:

## skonfigurować lokalne, zaufane CA na maszynie CA,

Generowanie klucza prywatnego urzędu certyfikacji wykonujemy komendą:

openssl ecparam -out ca.key -name prime256v1 –genkey

Wygenerowanie żądania podpisania certyfikatu wykonujemy komedną:

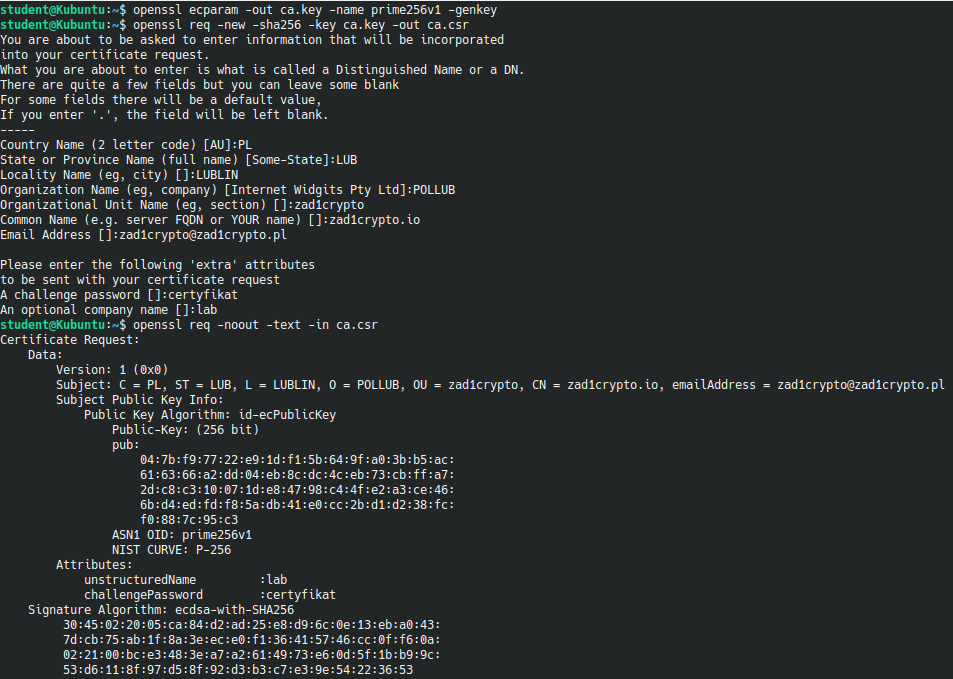
openssl req -new -sha256 -key ca.key -out ca.csr

Certyfikujemy urząd certyfikacji certyfikatem komendą:

openssl x509 -req -sha256 -days 365 -in ca.csr -signkey ca.key -out ca.crt

Weryfikujemy żądanie komendą:

openssl req -noout -text -in ca.csr



## wygenerować i podpisać certyfikat dla serwera Apache,

Generujemy klucz dla certyfikatu serwera komendą:

openssl ecparam -out server.key -name prime256v1 –genkey

Generujemy żądanie podpisania certyfikatu komendą:

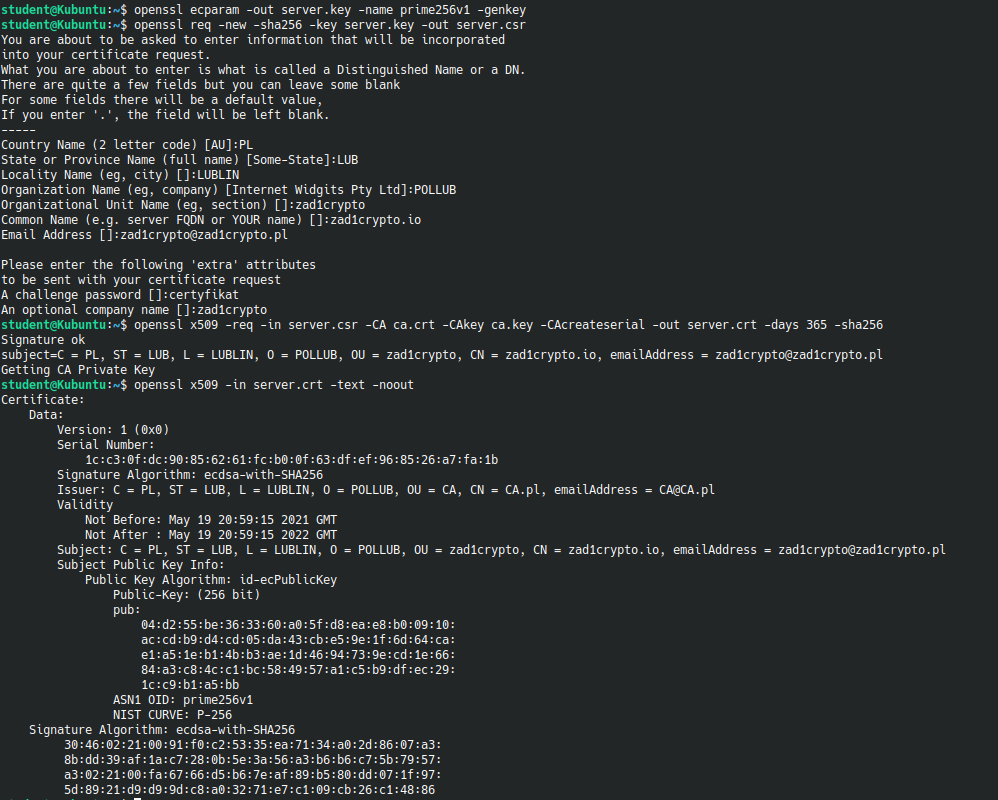
openssl req -new -sha256 -key server.key -out server.csr

Generujemy certyfikat komendą:

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 365 -sha256

Weryfikujemy dane certyfikatu:

openssl x509 -in server.crt -text -noout

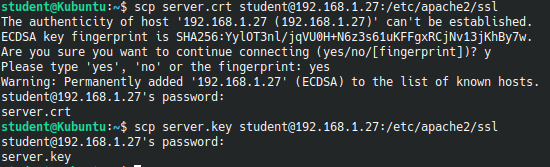


## dokonać dystrybucji certyfikatu z zachowaniem maksymalnego bezpieczeństwa,

Przenosimy certyfikat i klucz do serwera komendami:

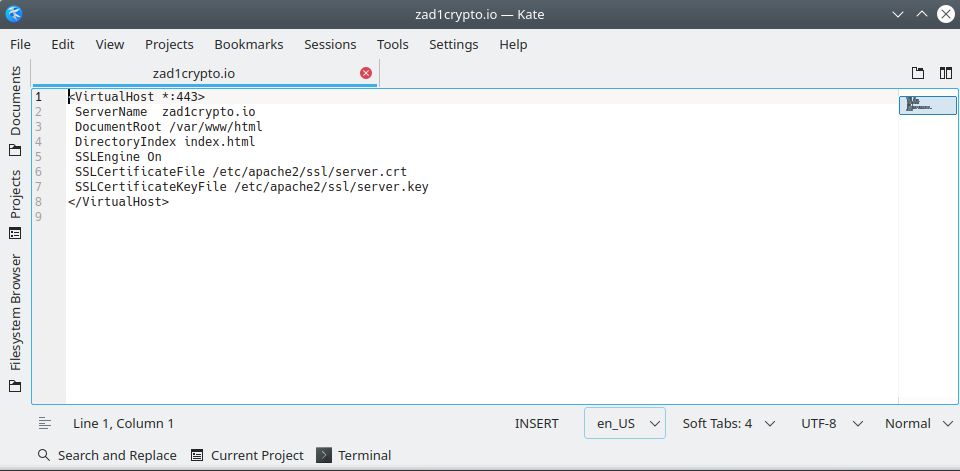
scp server.crt student@192.168.1.27:/etc/apache2/ssl

scp server.key student@192.168.1.27:/etc/apache2/ssl

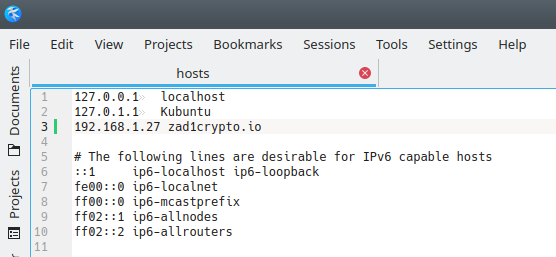


## skonfigurować serwer Apache do realizacji WYŁĄCZNIE bezpiecznych połączeń SSL,

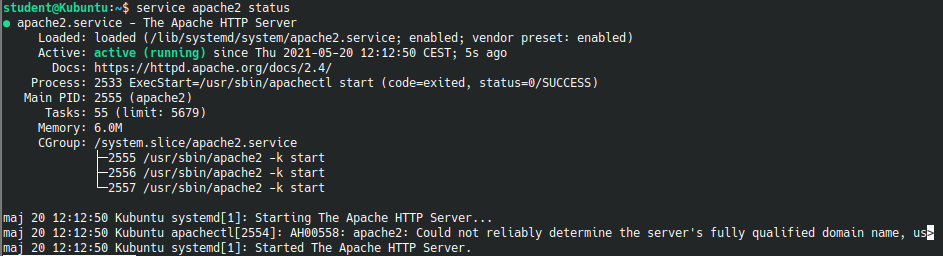
Konfigurujemy serwer Apache:



Dodajemy domenę do listy:

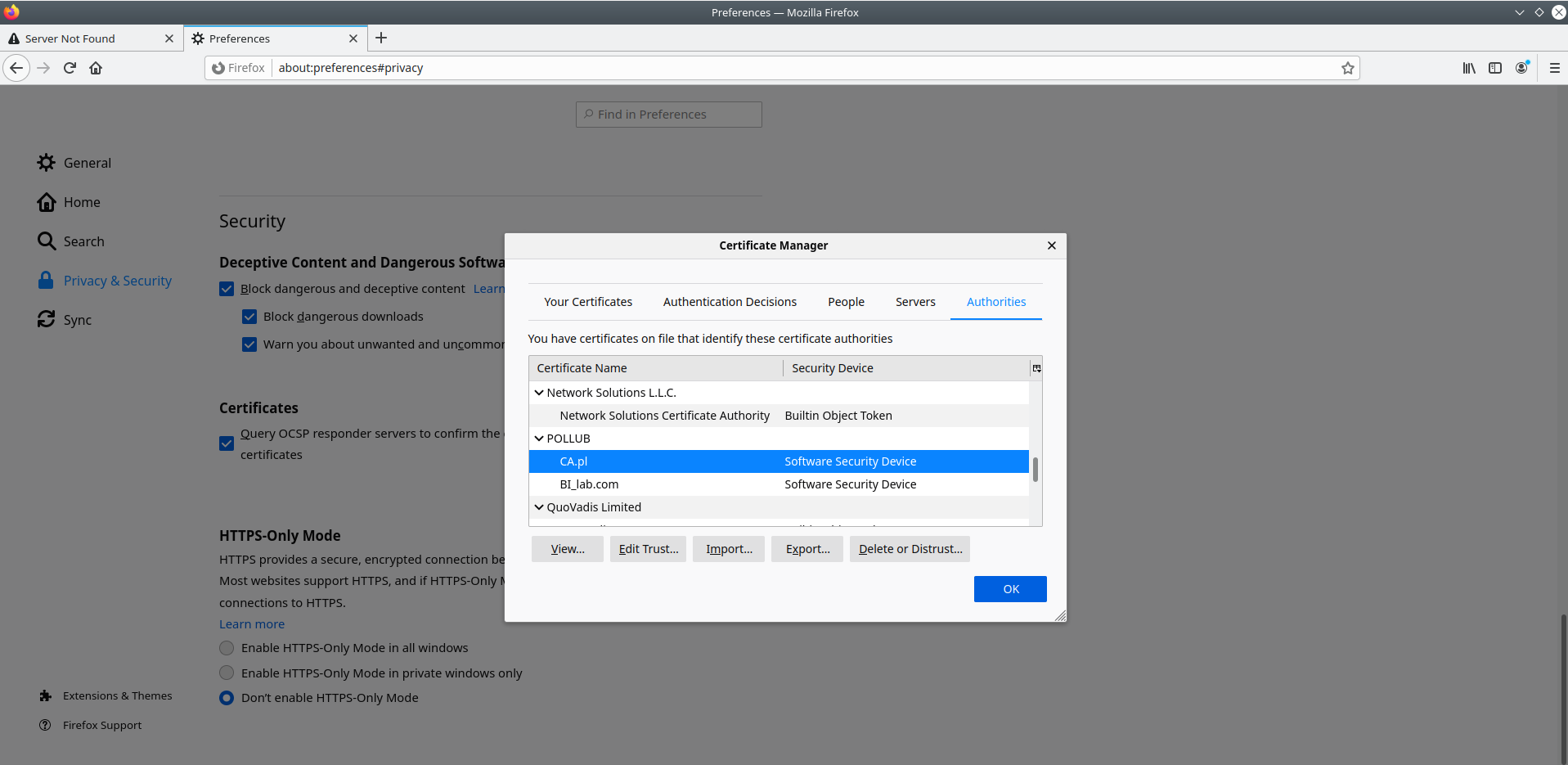


Sprawdzamy status serwera:



## skonfigurować przeglądarkę internetową do wykorzystania bezpiecznego połączenia SSL,

Dodajemy certyfikat urzędu certyfikacji do przeglądarki:



## potwierdzić poprawność zrealizowanej konfiguracji przez zalogowanie się na serwerze Apache z przeglądarki działającej na maszynie client.