Nginx

Zadanie

Cel:

Bezpieczna konfiguracja serwera webowego
Proszę przygotować konfigurację dla serwera Apache ORAZ Nginx spełniające następujące kryteria:

Zadanie 2: (kontynuacja zadania 1)

Proszę przygotować dwa certyfikaty klienckie dla certyfikatu serwera z Zadania 1 p.1 - User A, User B
Ścieżka /only-user-a (wraz ze wszystkimi pod ścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem User A
Ścieżka /only-user-b(wraz ze wszystkimi pod ścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem User B
Ścieżka /user-a-or-b(wraz ze wszystkimi pod ścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem User A lub User B
(punkt dodatkowy, nieobowiązkowy) Podścieżka /info dla ścieżek z p. 2,3,4 (czyli np. /only-user-a/info) wyświetli informacje o użytkowniku odczytane z jego certyfikatu klienckiego.

Środowisko pracy:

Ubuntu 20.04 Virtualbox, Docker

Przebieg ćwiczenia Nginx

W zadaniu tym wykorzystano już istniejące pliki z poprzedniego zadania. Niektóre parametry i komendy trzeba było zmienić, aby móc wykonać zadanie drugie. Również rozbudowano dockerfile.

Tworzenie kluczy i certyfikatów

Pierwszym krokiem było wygenerowanie certyfikatow CA za pomocą komendy:

```
openssl req -newkey rsa:2048 -nodes -keyform PEM -keyout
selfsigned-ca.key -x509 -days 3650 -outform PEM -out
selfsigned-ca.crt
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl req -newkey rsa:2048 -nodes -keyform PEM -keyout nginx-ca.key -x509 -days 3650    -outform PEM -out nginx-ca.crt
Generating a RSA private key
....+++++
.............+++++
writing new private key to 'nginx-ca.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]:Polska
Locality Name (eg, city) []:Wroclaw
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Pwr
Organizational Unit Name (eg, section) []:CBE
Common Name (e.g. server FQDN or YOUR name) []:kliencinginx
Email Address []:242027@student.pwr.edu.pl
milosz@milosz-VirtualBox:~/2nginx$
```

Jak widać powyżej uzupełniono już parametry informacyjne.

Następnie wygenerowano klucz serwera dla serwera o nazwie selfsigned.key.

```
openssl genrsa -out selfsigned.key 2048
```

```
Email Address []:242027@student.pwr.edu.pl
milosz@milosz-VirtualBox:~/2nginx$ openssl genrsa -out selfsigned.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
milosz@milosz-VirtualBox:~/2nginx$
```

Potem stworzono certyfikat selfsigned.crt. Z hasłem ”milosz”.

```
openssl req -new -key selfsigned.key -out selfsigned.csr
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl req -new -key selfsigned.key -out selfsigned.csr
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]:Polska
Locality Name (eg, city) []:Wroclaw
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Pwr
Organizational Unit Name (eg, section) []:CBE
Common Name (e.g. server FQDN or YOUR name) []:kliencinginx
Email Address []:242027@student.pwr.edu.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:milosz
An optional company name []:milosz
```

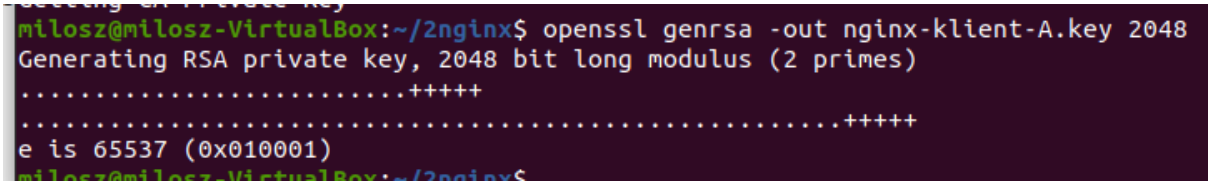
Następnie wykonano podpis CSR dla nginx.

```
openssl x509 -req -in selfsigned.csr -CA nginx-ca.crt -CAkey
nginx-ca.key -set_serial 100 -days 365 -outform PEM -out
selfsigned.crt
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl x509 -req -in selfsigned.csr -CA nginx-ca.crt -CAkey nginx-ca.key -set_serial 100 -days 365 -outform PEM -out selfsigned.crt
Signature ok
subject=C = PL, ST = Polska, L = Wroclaw, O = Pwr, OU = CBE, CN = kliencinginx, emailAddress = 242027@student.pwr.edu.pl
Getting CA Private Key
```

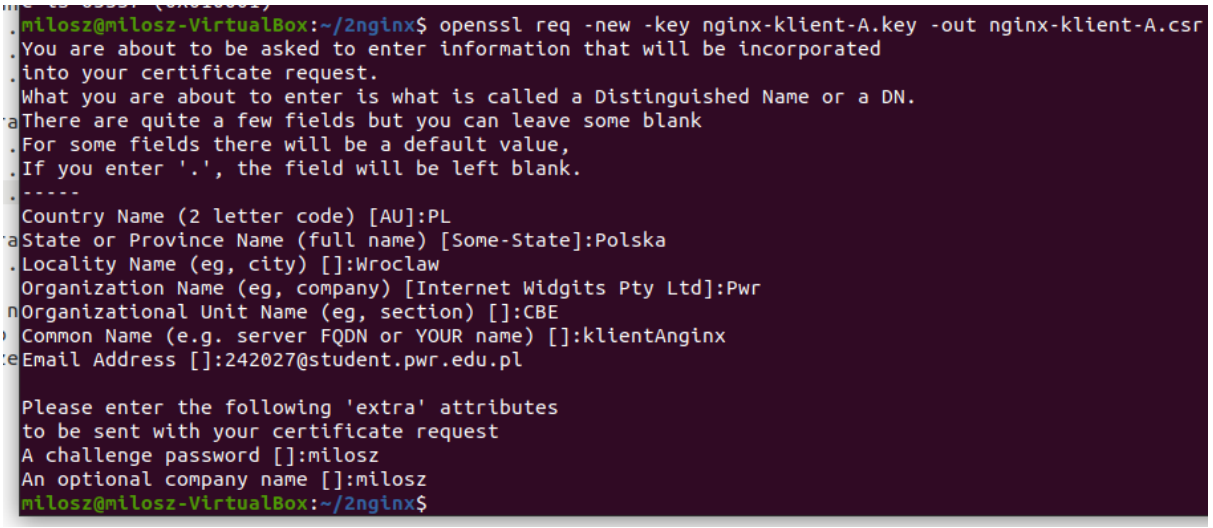
Później przystąpiono do zrobienia podwójnego uwierzytelniania dla klientów. Pierwszy krok na tym etapie to stworzenie certyfikatów i kluczy klienckich. Poniżej polecenie:

```
openssl genrsa -out nginx-client-A.key 2048
```

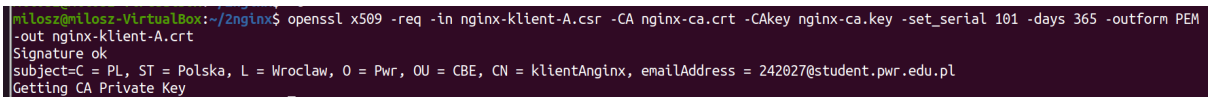


CSR dla klienta A:

```
openssl req -new -key nginx-klient-A.key -out
nginx-klient-A.csr
```

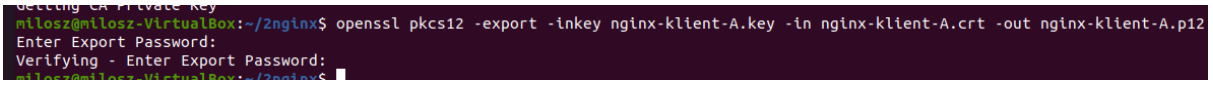



```
openssl x509 -req -in nginx-klient-A.csr -CA nginx-ca.crt
-CAkey nginx-ca.key -set_serial 101 -days 365 -outform PEM
-out nginx-klient-A.crt
```



Ostatni krok to połączenie certyfikatu klienta i klucza klienta A w pakiet .p12. Potrzebny jest on dla użytkownika, aby ten mógł potwierdzić swoją tożsamość wchodząc na ścieżkę w przeglądarce. Wpisano hasło miłosz. Polecenie:

```
openssl pkcs12 -export -inkey nginx-klient-A.key -in
nginx-klient-A.crt -out nginx-klient-A.p12
```



Takie same kroki wykonano dla klienta B tylko, certyfikaty i klucze przypisane zostały pod klienta B.

```
openssl genrsa -out nginx-klient-B.key 2048
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl genrsa -out nginx-klient-B.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................................
.....................................................................+++++
e is 65537 (0x010001)
```

```
openssl req -new -key nginx-klient-B.key -out
nginx-klient-B.csr
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl req -new -key nginx-klient-B.key -out nginx-klient-B.csr
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]:Polska
Locality Name (eg, city) []:Wroclaw
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Pwr
Organizational Unit Name (eg, section) []:CBE
Common Name (e.g. server FQDN or YOUR name) []:klientBnginx
Email Address []:242027@student.pwr.edu.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:milosz
An optional company name []:milosz
milosz@milosz-VirtualBox:~/2nginx$
```

```
openssl x509 -req -in nginx-klient-B.csr -CA nginx-ca.crt
-CAkey nginx-ca.key -set_serial 102 -days 365 -outform PEM
-out nginx-klient-B.crt
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl x509 -req -in nginx-klient-B.csr -CA nginx-ca.crt -CAkey nginx-ca.key -set_seri
al 102 -days 365 -outform PEM -out nginx-klient-B.crt
Signature ok
subject=C = PL, ST = Polska, L = Wroclaw, O = Pwr, OU = CBE, CN = klientBnginx, emailAddress = 242027@student.pwr.edu.pl
Getting CA Private Key
```

```
openssl pkcs12 -export -inkey nginx-klient-B.key -in
nginx-klient-B.crt -out nginx-klient-B.p12
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl pkcs12 -export -inkey nginx-klient-B.key -in nginx-klient-B.crt -out nginx-klient-B.p12
Enter Export Password:
Verifying - Enter Export Password:
milosz@milosz-VirtualBox:~/2nginx$
```

Koniec generowania certyfikatów

Po utworzeniu certyfikatów i kluczy kliencki przystąpiono do edycji i konfiguracji dockerfile i pliku nginx.conf. Była to bardzo wymagająca praca poprzez metodę prób i błędów i studiowanie dokumentacji nginx.

Konfiguracja pliku nginx.conf

Wskazano ścieżkę na nasz wygenerowany certyfikat CA i włączono opcję, aby klienci byli opcjonalnie tzn. tylko do wymaganych ścieżek.

```
ssl_client_certificate /etc/ssl/certs/nginx-selfsigned-ca.crt;
ssl_verify_client optional;
```

```
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
ssl_client_certificate /etc/ssl/certs/nginx-selfsigned-ca.crt;
ssl_verify_client on;
```

Następnie przystąpiono do konfiguracji ścieżek i pod ścieżek. Na początku próbowano na podstawie klienta *if ($ssl_client_s_dn_cn != 'UserA'){ return 403;}*, ale zmieniono to na fingerprint SHA1 certyfikatów i to wyszło. Dlatego jest wiele opcji sprawdzenia klientów. Potem stworzono instrukcje warunkowe. Jednak wpierw trzeba było zdobyć fingerprint SHA1 certyfikatów. Wykonuje się to poleceniem:

```
openssl x509 -in przyklad.crt -noout -fingerprint
```

Sprawdzenie klienta A

```
openssl x509 -in nginx-klient-A.crt -noout -fingerprint
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl x509 -in nginx-klient-A.crt -noout -fingerprint
SHA1 Fingerprint=7E:0D:6F:4E:C8:31:91:DB:76:9C:5C:0A:84:4B:BC:AC:47:94:F4:81
milosz@milosz-VirtualBox:~/2nginx$
```

Sprawdzenie klienta B

```
openssl x509 -in nginx-klient-B.crt -noout -fingerprint
```

```
milosz@milosz-VirtualBox:~/2nginx$ openssl x509 -in nginx-klient-B.crt -noout -fingerprint
SHA1 Fingerprint=BB:FF:4B:5F:32:D3:32:70:FB:7C:AF:AA:C3:EB:C1:66:6A:B2:DD:4B
milosz@milosz-VirtualBox:~/2nginx$
```

Fingerprint SHA1 klienta A: `7e0d6f4ec83191db769c5c0a844bbcac4794f481`
Fingerprint SHA1 klienta B: `bbff4b5f32d33270fb7cafaac3ebc1666ab2dd4b`

only-user-a

```
location /only-user-a {
#         root /var/www/html/only-user-a;
if                  ($ssl_client_fingerprint                  !=
7e0d6f4ec83191db769c5c0a844bbcac4794f481) {
                              return 403;
                          }
                      }
```

only-user-b

```
location /only-user-b {
#         root /var/www/html/only-user-b;
```

```
if                  ($ssl_client_fingerprint                    !=
bbff4b5f32d33270fb7cafaac3ebc1666ab2dd4b) {
                            return 403;
                            }
                }
```

user-a-or-b

```
location /user-a-or-b {
#    root /var/www/html/user-a-or-b;
           if ($ssl_reject) {
                               return 403;
                            }
                }
```

Kolejny etap to dodanie map, ponieważ umożliwia tworzenie zmiennych w pliku konfiguracyjnym nginx.conf, których wartości są warunkowe — to znaczy zależą od wartości innych zmiennych.

```
     map  $ssl_client_fingerprint $ssl_reject {
         default 1;
         c4cb2ee3c2e8dcdb5f2b0d516e1bcd4e70f69d31 0;
         1757787e0ea2296dd0dd729d27dc1dbf546f7583 0;
         }
```

Konfiguracja dockerfile nginx

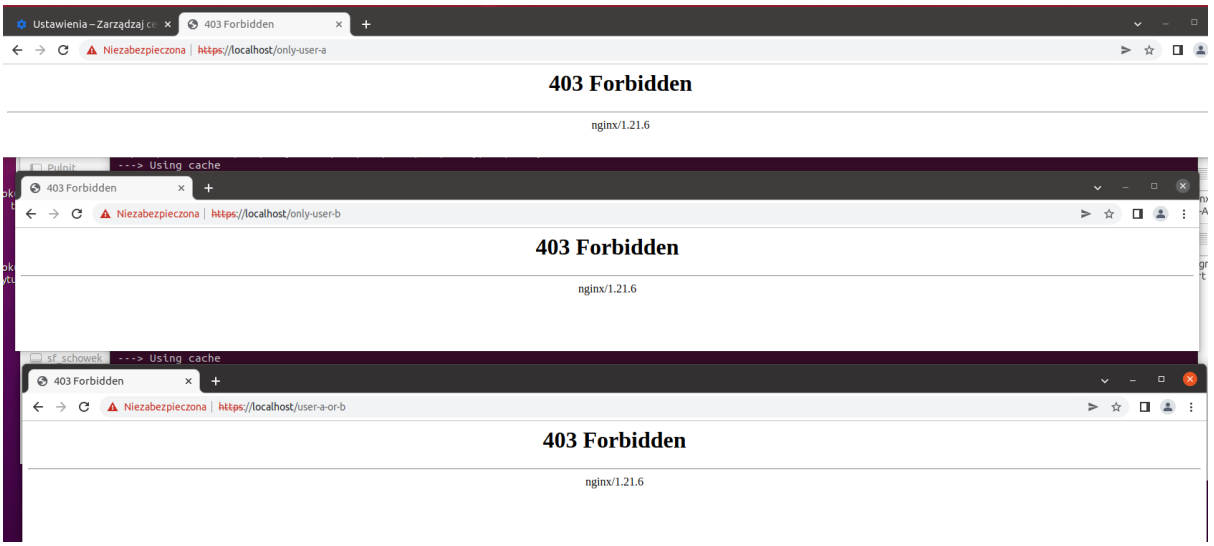
Do dockerfile trzeba było dodać tylko nowe katalogi podstrony .html oraz zapisać nasz plik konfiguracyjny nginx.conf przed odpaleniem dockera.

```
#wgranie katalogów dla klientow
RUN mkdir /var/www/html/only-user-a
RUN mkdir /var/www/html/only-user-b
RUN mkdir /var/www/html/user-a-or-b

#wgranie klientow plikow html
COPY ./indexklientA.html /var/www/html/only-user-a/index.html
COPY ./indexklientB.html /var/www/html/only-user-b/index.html
COPY ./indexklientAiB.html
/var/www/html/user-a-or-b/index.html

# wgranie wygenerowanych wcześniej kluczy i certyfikatu
COPY ./selfsigned.key /etc/ssl/private/nginx-selfsigned.key
COPY ./selfsigned.crt /etc/ssl/certs/nginx-selfsigned.crt
COPY ./nginx-ca.crt /etc/ssl/certs/nginx-selfsigned-ca.crt
```

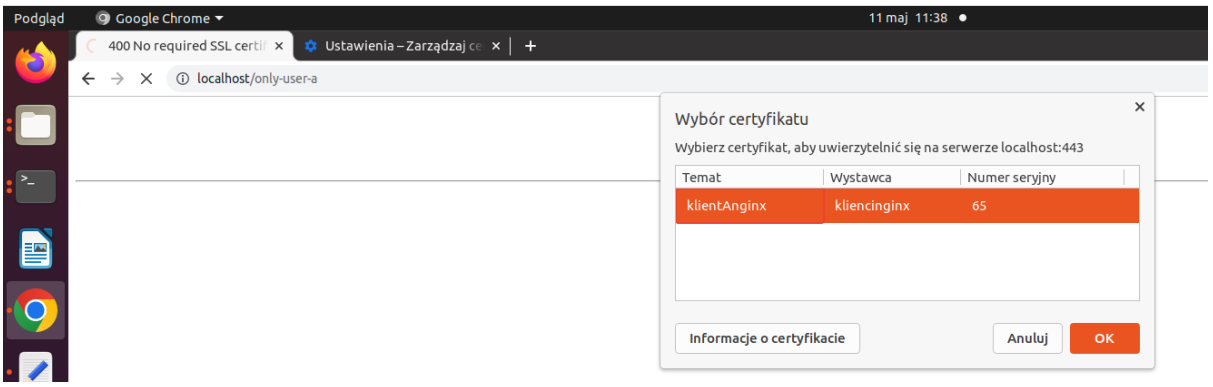
Następnie odpalono obraz nginx

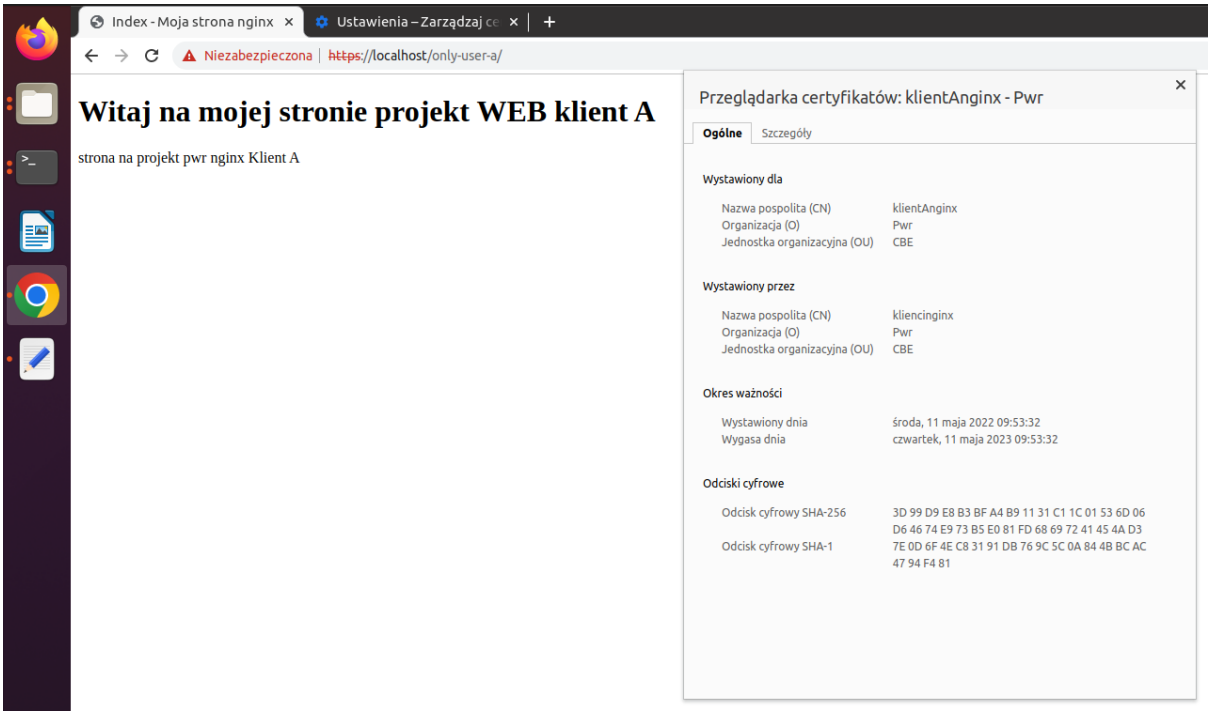
Przedstawienie działania certyfikatów i kluczy klienckich

Na ten moment nie dodano jeszcze certyfikatów w przeglądarce, aby pokazać brak dostępu do wyznaczonych ścieżek.

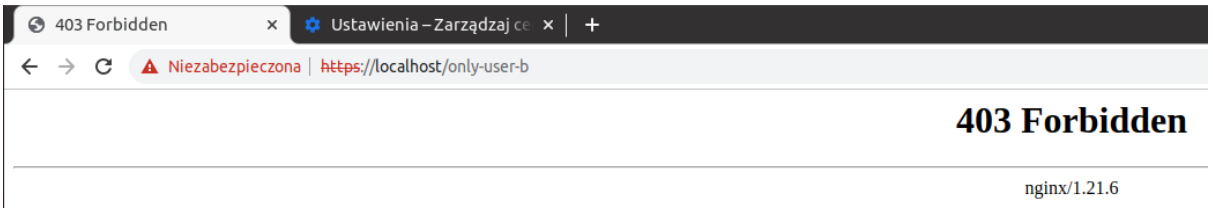


Klient A



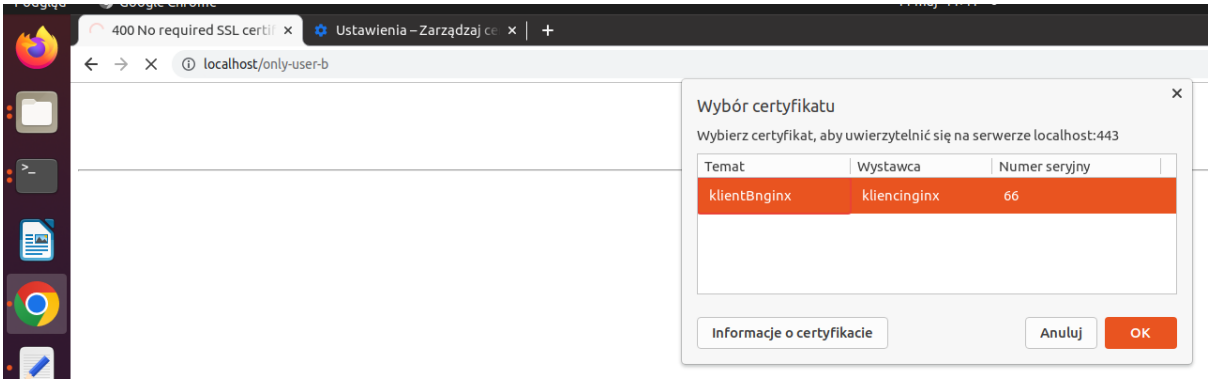

Index - Moja strona nginx
Ustawienia – Zarządzaj ce
Niezabezpieczona | https://localhost/only-user-a/
Witaj na mojej stronie projekt WEB klient A
strona na projekt pwr nginx Klient A
Przeglądarka certyfikatów: klientAnginx - Pwr
Ogólne
Szczegóły
Wystawiony dla
Nazwa pospolita (CN) klientAnginx
Organizacja (O) Pwr
Jednostka organizacyjna (OU) CBE
Wystawiony przez
Nazwa pospolita (CN) klienciginx
Organizacja (O) Pwr
Jednostka organizacyjna (OU) CBE
Okres ważności
Wystawiony dnia środa, 11 maja 2022 09:53:32
Wygasa dnia czwartek, 11 maja 2023 09:53:32
Odciski cyfrowe
Odcisk cyfrowy SHA-256 3D 99 D9 E8 B3 BF A4 B9 11 31 C1 1C 01 53 6D 06 D6 46 74 E9 73 B5 E0 81 FD 68 69 72 41 45 4A D3
Odcisk cyfrowy SHA-1 7E 0D 6F 4E C8 31 91 DB 76 9C 5C 0A 84 4B BC AC 47 94 F4 81

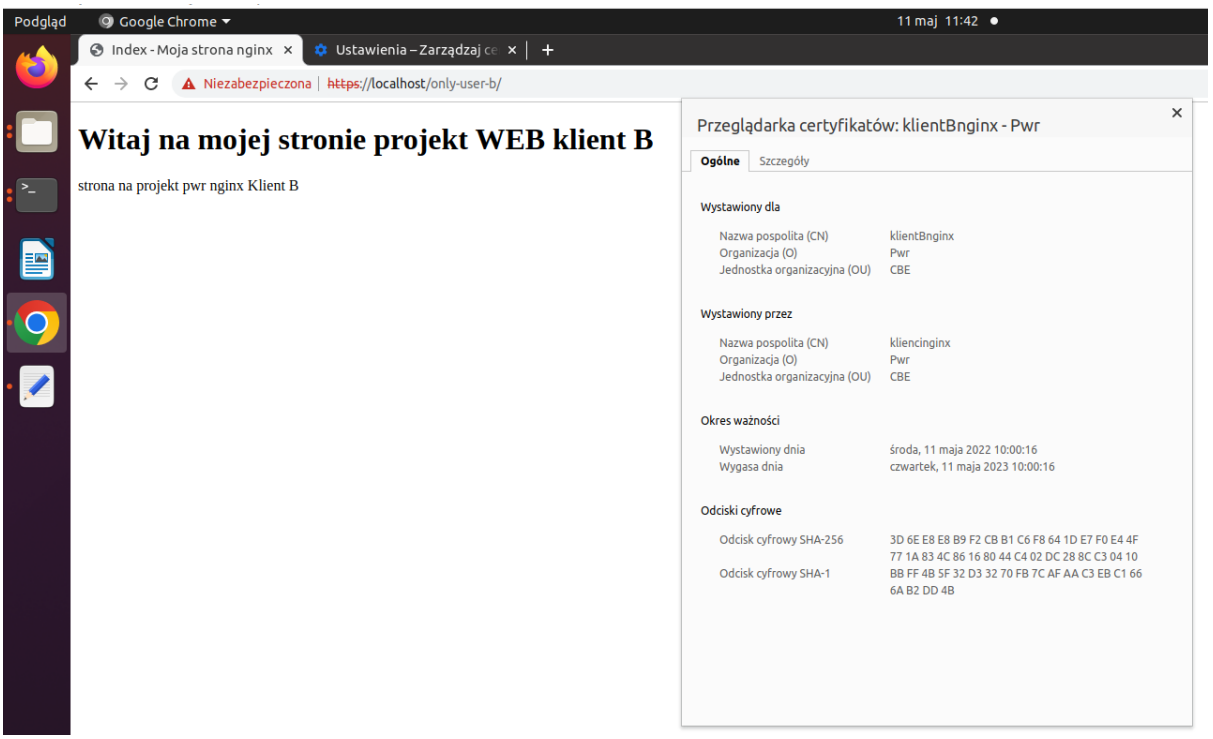

Podgląd
Google Chrome
Index - Moja strona nginx
Ustawienia – Zarządzaj ce
Niezabezpieczona | https://localhost/only-user-a/index.html
Witaj na mojej stronie projekt WEB klient A
strona na projekt pwr nginx Klient A

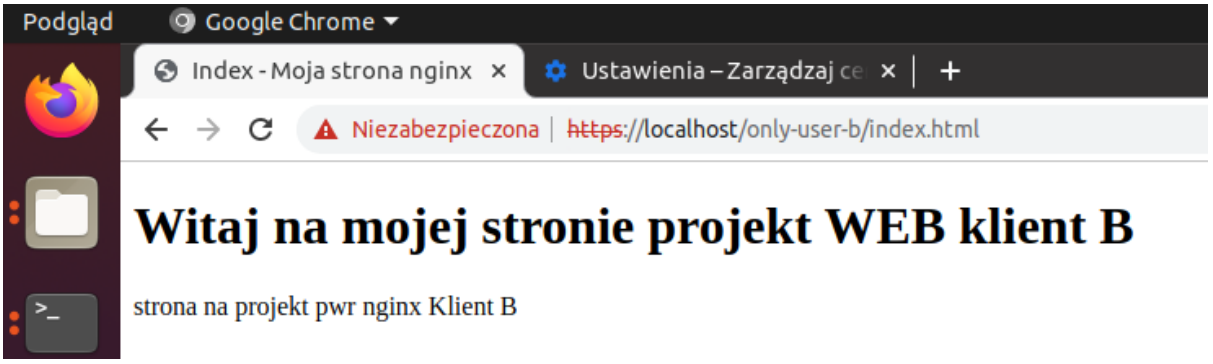

403 Forbidden
Ustawienia – Zarządzaj ce
Niezabezpieczona | https://localhost/only-user-b
403 Forbidden
nginx/1.21.6

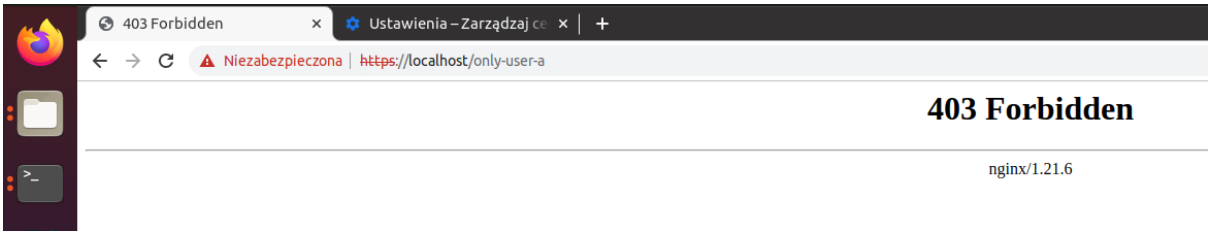

Niezabezpieczona | https://localhost/user-a-or-b/
Witaj na mojej stronie projekt WEB klient A i B
strona na projekt pwr nginx Klient A i B

Klient B


400 No required SSL certif
Ustawienia – Zarządzaj ce
localhost/only-user-b
Wybór certyfikatu
Wybierz certyfikat, aby uwierzytelnić się na serwerze localhost:443
Temat
Wystawca
Numer seryjny
klientBnginx
kliencinginx
66
Informacje o certyfikacie
Anuluj
OK

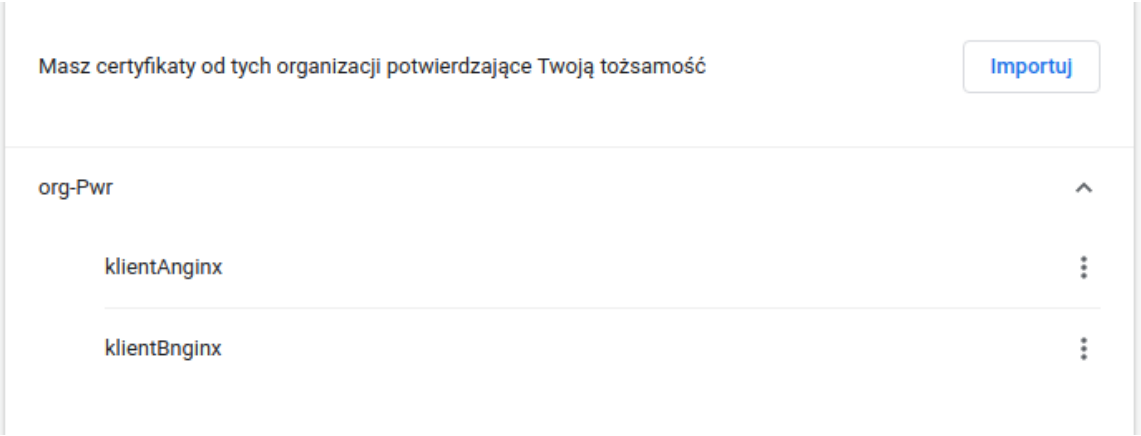

Podgląd
Google Chrome
11 maj 11:42
Index - Moja strona nginx
Ustawienia – Zarządzaj ce
Niezabezpieczona
https://localhost/only-user-b/
Witaj na mojej stronie projekt WEB klient B
strona na projekt pwr nginx Klient B
Przeglądarka certyfikatów: klientBnginx - Pwr
Ogólne
Szczegóły
Wystawiony dla
Nazwa pospolita (CN) klientBnginx
Organizacja (O) Pwr
Jednostka organizacyjna (OU) CBE
Wystawiony przez
Nazwa pospolita (CN) kliencinginx
Organizacja (O) Pwr
Jednostka organizacyjna (OU) CBE
Okres ważności
Wystawiony dnia środa, 11 maja 2022 10:00:16
Wygasa dnia czwartek, 11 maja 2023 10:00:16
Odciski cyfrowe
Odcisk cyfrowy SHA-256 3D 6E E8 E8 B9 F2 CB B1 C6 F8 64 1D E7 F0 E4 4F 77 1A 83 4C 86 16 80 44 C4 02 DC 28 8C C3 04 10
Odcisk cyfrowy SHA-1 BB FF 4B 5F 32 D3 32 70 FB 7C AF AA C3 EB C1 66 6A B2 DD 4B


Podgląd
Google Chrome
Index - Moja strona nginx
Ustawienia – Zarządzaj ce
Niezabezpieczona
https://localhost/only-user-b/index.html
Witaj na mojej stronie projekt WEB klient B
strona na projekt pwr nginx Klient B

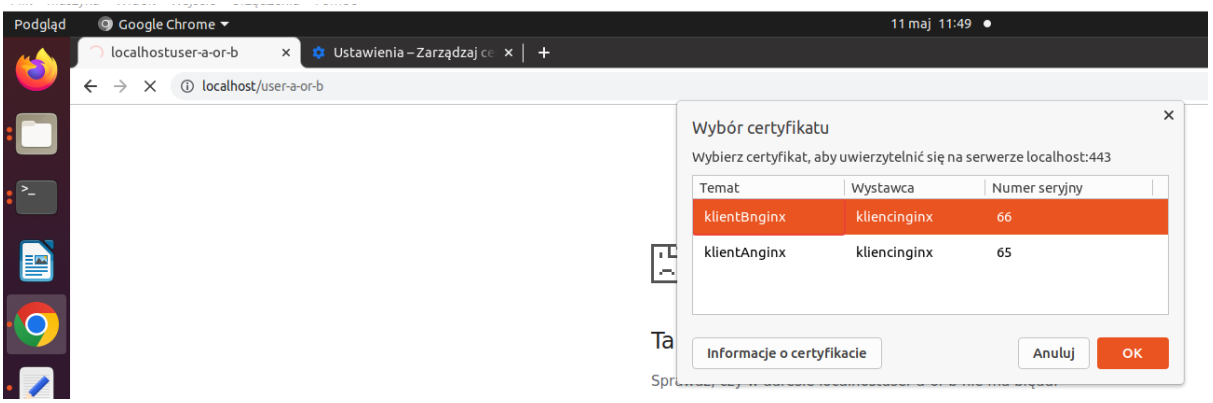


Dwa certyfikaty zaimportowane równolegle.

Poniżej zaimportowano dwa certyfikaty do przeglądarki.



Użytkownik wybiera, z którego klienckiego certyfikatu chcę korzystać, aby przejść. Jednak wtedy nie potrzeba robić kilku certyfikatów, ale jeden. Pokazano to dla przykładu,, że można importować dwa certyfikaty.



Podsumowanie

Konfiguracja nginx zajęła bardzo wiele czasu, więcej od Apache, ale udało się osiągnąć cel. Największy problem był ze wskazaniem parametru klienta, dlatego zmieniono na fingerprint, a nie na nazwę klienta.