Security: PKI

Do realizacji zadania wykorzystano WSL1 na systemie Windows 2019 server.
Dystrybucja uruchomiona pod systemem WSL to Ubuntu 22.04.4 LTS

Tworzenie prostego Urzędu Certyfikacyjnego (Certification Authority)

Kolejno wykonaj następujące działania:
cd /usr/lib/ssl/misc/
./CA.pl -newca
Po uruchomieniu skryptu CA.pl wprowadź:
podaj nazwę pliku CA: <Enter>
podaj pass phrase:
Country name: PL
State or provice Name: Mazowsze
Locality name (eg. city): Warszawa
Organization Name (eg. company): WWSI
Organization Unit Name: (eg. section): Zakład Sieci Teleinformatycznych (wpisane: ZST)
Common Name (e.g. server FQDN lub twoje imie): Robert
Email address: rj@wwsi.edu.pl
A challenge password:
An optional company name:<Enter>
Enter pass phrase for ./demoCA/private/cakey.pem:

Realizacja

```
root@WSL:~> cd /usr/lib/ssl/misc/
root@WSL:misc> ./CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
.+.+..+......+....+..+.........+....+...+.................+.+.........+.....
.......+......+..+......+..........+
......+.....+.........+..........+..+.........+....+..+....+...+..+...+...+.
...........+...+....+...+...+.......
........+..+...+....+.....++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++*.....+...+..+.......
.........+...+.........+...+.........+........+.+......+...+...++++++++++++
++++++++++++++++++++++++++++++++++
++++++++++++++*..........+...+..+.+...+.........+...+.....+............+.
.+...+....+.....+...........+......
```

```
....+.....+.+.........+...+..+.+..+...........+....+.....+.........+..+...
...........+....+........+.......+.
....+...+...........+......+.......+..+.........+....++++++++++++++++++++
++++++++++++++++++++++++++++++++++
+++++++
..+........+....+...+.................+...++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++*....
..........+.........+.........+.......++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++*..+....
...+..+.+.................+.+.....+....+...........+.....+....+...........
..+...+..............+...+.+...+...
+..+.+..+.......+..........+.+......+...+......+...+........+.......+...+..
...+..........+...+..+++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Mazowsze
Locality Name (eg, city) []:Mińsk Mazowiecki
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ostrowski.net.pl
Organizational Unit Name (eg, section) []:self employed
Common Name (e.g. server FQDN or YOUR name) []:Kacper
Email Address []:kacper@ostrowski.net.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
==> 0
====
====
openssl ca  -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -
keyfile ./demoCA/private/cakey.pem -selfs
ign -extensions v3_ca -infiles ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number:
08:c9:1a:9f:b4:b4:cc:7f:79:5d:52:6e:21:df:72:35:1f:f5:66:11
Validity
Not Before: Jun  8 11:42:42 2025 GMT
```

```
Not After : Jun  7 11:42:42 2028 GMT
Subject:
countryName               = PL
stateOrProvinceName       = Mazowsze
organizationName          = ostrowski.net.pl
organizationalUnitName    = self employed
commonName                = Kacper
emailAddress              = kacper@ostrowski.net.pl
X509v3 extensions:
X509v3 Subject Key Identifier:
7E:7B:CD:64:8C:56:FE:B4:49:6E:D3:B8:FD:8E:64:63:E4:D4:D3:B3
X509v3 Authority Key Identifier:
7E:7B:CD:64:8C:56:FE:B4:49:6E:D3:B8:FD:8E:64:63:E4:D4:D3:B3
X509v3 Basic Constraints: critical
CA:TRUE
Certificate is to be certified until Jun  7 11:42:42 2028 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
```

Żądanie wydania certyfikatu X.509

Napisz składnię polecenia openssl służącego do wygenerowania żądania wydania nowego certyfikatu cyfrowego dla pary kluczy RSA o długości 2048 bitów. Zapamietaj klucz prywatny w pliku a_rsakey.pem a samo żądanie w pliku a_certreq.pem. Podpowiedź: użyj komendy req).

Sprawdź żądanie wydania certyfikatu poprzez wykonanie poniższego polecenia:
openssl req -in a_certreq.pem -text -noout
Teraz użytkownik maszyny A może przesłać do użytkownika maszyny C (gdzie zlokalizowany jest Urząd Certyfikacyjny) żądanie wydania certyfikatu zawarte w pliku a_certreq.pem. Napisz składnię polecenia (I wykonaj je) służącego do wydania certyfikatu X.509 na podstawie żądania wydania certyfikatu użytkownika A. Certyfikat zapisz w pliku a_cert.pem. openssl ca ... Po wprowadzeniu polecenia na ekranie pojawi się komunikat: Enter pass phrase for ./demoCA/private/cakey.pem

Realizacja

```
root@WSL:misc> openssl req -new -newkey rsa:2048 -keyout a_rsakey.pem -out
a_certreq.pem
.+.....+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++*.................+....+...+...+...+.........+......++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++*..+........+.......+...+......
.....+...+.+.....+......+...+...+...+....+..+.........+....+..+...+...+.....
..+......+.........+.....+................+.............+............+.....
........+......+..+.........+.+..+...+.......++++++++++++++++++++++++++++++
```

```
++++++++++++++++++++++++++++++++
..+......+.+........+......++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++*.+........+.......+...+...+.....+...+..........+........+.
....+.+........+......++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++*.............++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Mazowsze
Locality Name (eg, city) []:Mińsk Mazowiecki
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ostrowski.net.pl
Organizational Unit Name (eg, section) []:self employed
Common Name (e.g. server FQDN or YOUR name) []:Kacper
Email Address []:kacper@ostrowski.net.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Q@wertyuiop
An optional company name []:
root@WSL:misc> openssl req -in a_certreq.pem -text -noout
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = PL, ST = Mazowsze, L = Mi\C3\85\C2\84sk Mazowiecki, O =
ostrowski.net.pl, OU = self employed, CN = Kacper, emailAddress =
kacper@ostrowski.net.pl
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ea:a3:10:54:c6:04:98:db:f1:33:d4:89:f3:61:
8c:01:9a:3c:e5:3f:88:29:52:cc:17:05:7d:2b:a2:
52:68:a2:7f:d8:f8:ce:81:09:87:4b:75:fd:dd:eb:
66:ba:c3:6f:bc:b9:70:80:64:ee:75:c5:ef:6b:97:
65:79:1d:01:53:df:d5:d0:75:ad:92:94:64:83:c3:
29:fe:2f:bc:be:3d:9e:53:c1:e2:39:78:c2:2f:21:
0c:bc:71:a7:6e:b1:d9:05:11:48:98:33:e7:d8:cb:
6f:d3:30:1e:d7:30:ca:8e:5d:32:ba:be:3e:e2:93:
86:83:5f:31:6c:61:ce:6a:19:79:67:04:5c:f0:90:
8c:41:8d:ea:8f:e5:1b:53:96:c3:49:8d:a9:02:66:
a3:3c:44:03:a2:e2:34:c4:50:78:35:46:d7:ef:e8:
23:de:c9:a7:8a:af:ce:47:89:f4:17:c9:b1:63:62:
```

```
64:ba:09:a5:78:b1:f3:a9:ad:d4:9f:89:71:8a:fc:
eb:53:8b:8e:80:be:1e:f8:bc:f2:6c:45:ab:50:63:
5a:ca:8c:e9:17:15:10:9a:49:0a:8f:40:7d:31:28:
35:9f:e8:ab:3b:aa:9a:bc:cd:b4:88:45:4f:96:07:
57:51:fc:2c:a7:63:69:dc:72:3a:70:b7:1e:58:8c:
46:d1
Exponent: 65537 (0x10001)
Attributes:
challengePassword        :Q@wertyuiop
Requested Extensions:
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
b3:fc:3c:bc:eb:a1:95:c8:b6:9e:c5:a3:01:af:a6:d2:3e:b6:
c7:26:74:c2:4d:a8:11:39:fd:4f:69:c6:9c:20:cf:a1:2c:af:
47:67:64:87:ed:73:1f:aa:20:69:0b:9e:4f:7f:81:ec:fb:bf:
c9:c1:f9:8e:3d:a3:24:25:52:7d:51:58:cb:bd:46:63:ea:d1:
46:13:a5:42:aa:3c:19:4a:d3:54:01:d5:1a:1b:14:fe:64:d9:
45:1b:d4:cf:76:e3:94:3f:fc:a7:1c:50:9a:af:7e:5a:43:83:
2b:ed:f3:b0:9d:ce:e2:52:f9:cf:d1:6a:7b:de:f9:85:32:1f:
64:17:fe:33:68:b2:52:5d:bf:75:7e:20:4d:89:4c:2d:b4:77:
0e:dc:1b:cd:63:c6:0f:f2:26:12:3c:a1:03:c3:03:17:29:c7:
a3:49:1a:d2:3e:e0:1b:88:16:af:d1:67:37:62:2b:5e:72:77:
51:5a:32:d1:c6:41:d2:88:53:59:5f:b3:03:df:36:1e:1c:18:
a5:bb:00:a9:e1:45:57:28:74:4d:48:cb:db:c3:71:f9:69:1d:
a5:42:08:fa:45:2a:ca:c6:aa:b1:38:10:e6:8e:1a:30:26:61:
f1:a8:33:f1:f6:fa:56:1f:da:fc:7c:16:15:c7:86:7c:51:65:
9c:8e:2c:4e
# nie miałem dwóch maszyn żeby zrobić test natomiast widać że sygnatury są
poprawne
root@WSL:misc> openssl ca -in a_certreq.pem -out a_cert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
ERROR:There is already a certificate for
/C=PL/ST=Mazowsze/O=ostrowski.net.pl/OU=self
employed/CN=Kacper/emailAddress=kacper@ostrowski.net.pl
The matching entry has the following details
Type          :Valid
Expires on    :280607114242Z
Serial Number :08C91A9FB4B4CC7F795D526E21DF72351FF56611
File name     :unknown
Subject Name  :/C=PL/ST=Mazowsze/O=ostrowski.net.pl/OU=self
employed/CN=Kacper/emailAddress=kacper@ostrowski.net.pl
root@WSL:misc>
```

Pytania

Pytanie 1: Które pliki zostały zmodyfikowane w bazie danych „Test CA” na maszynie użytkownika C?

Po wydaniu certyfikatu przez Urząd Certyfikacji (CA), modyfikacji ulegają następujące pliki w katalogu demoCA:

- `index.txt` – plik bazy danych CA, zawierający informacje o wydanych certyfikatach.
- `serial` – plik przechowujący numer seryjny kolejnego certyfikatu.
- `newcerts/<numer>.pem` – nowo wygenerowany certyfikat użytkownika.

Te pliki są automatycznie aktualizowane przez polecenie `openssl ca`.

Polecenie do weryfikacji certyfikatu cyfrowego (na maszynie A)

Użytkownik maszyny A może zweryfikować certyfikat za pomocą poniższego polecenia:

```
openssl verify -CAfile cacert.pem a_cert.pem
```

gdzie:

- `cacert.pem` – certyfikat Urzędu Certyfikacji (CA),
- `a_cert.pem` – certyfikat użytkownika A, który ma zostać zweryfikowany.

Pytanie 2: Które dane są potrzebne do wykonania operacji weryfikacji certyfikatu cyfrowego?

Aby wykonać weryfikację certyfikatu cyfrowego, potrzebne są następujące dane:

- Certyfikat użytkownika, który ma zostać zweryfikowany (np. `a_cert.pem`).
- Certyfikat Urzędu Certyfikacji (np. `cacert.pem`), który wystawił podpisany certyfikat.
- (Opcjonalnie) Lista unieważnionych certyfikatów (CRL), jeśli weryfikacja ma uwzględniać unieważnienia.