

Ασφάλεια Πληροφοριακών Συστημάτων

3^η Άσκηση: Δημιουργία και
εγκατάσταση πιστοποιητικού Web
Server με τη χρήση του OpenSSL

Ακαδημαϊκό Έτος: 2022 – 2023

Ομάδα:



Μπουμπλίνη Αναστασία
(Π19117)



aboublini@gmail.com



ANASTASIA BOUBLINI
(p19117@unipi.gr)



Μπριστογιάννης
Ιωακείμ (Π19048)



ioakeim13@hotmail.gr



IOAKEIM EL-KHATTAB-
BRISTOGIANNIS
(p19048@unipi.gr)



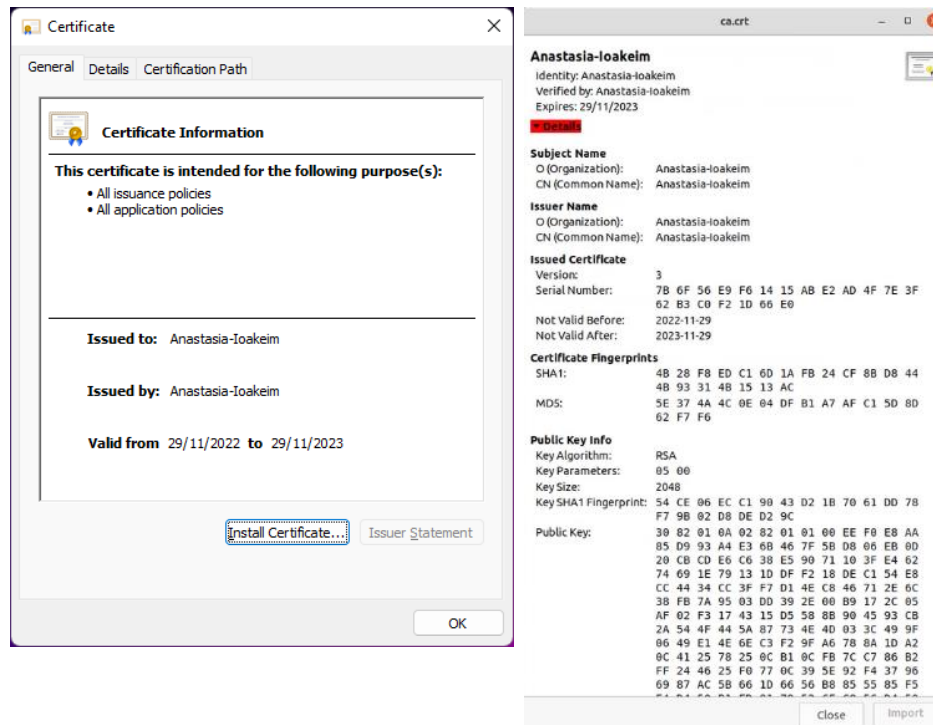
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Πίνακας Περιεχομένων

1.	Δημιουργία ΑΠ.....	3
2.	Δημιουργία και Πιστοποίηση Κλειδιών για Server.....	4
3.	Δημιουργία, πιστοποίηση και ανάκληση κλειδιών	6
4.	Εισαγωγή Πιστοποιητικού στον Server	8
5.	Διαμόρφωση του Server για διπλή αυθεντικοποίηση	8

1. Δημιουργία ΑΠ

Δημιουργήθηκε το παρακάτω αυτό-υπογεγραμμένο πιστοποιητικό (Εικόνες 1 & 2) σε περιβάλλον Linux κάνοντας χρήση του OpenSSL. Ακολουθήθηκε η διαδικασία που φαίνεται στην Εικόνα 3.



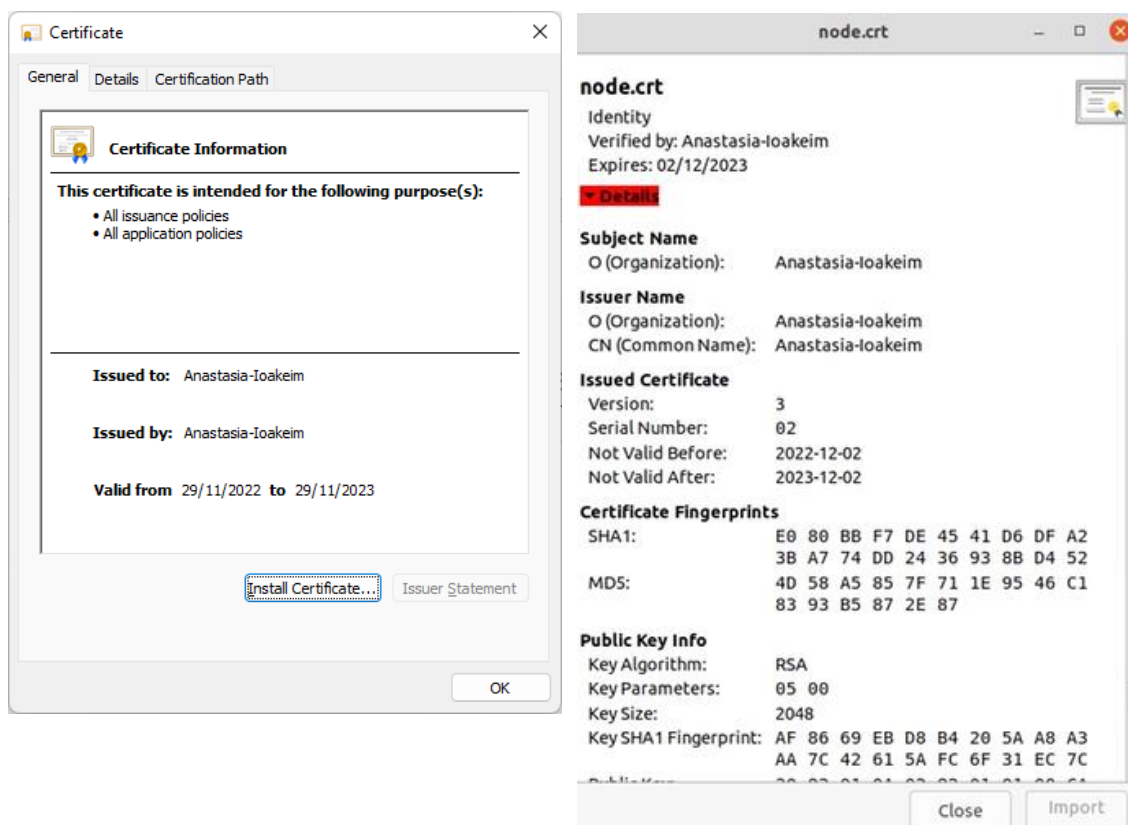
Εικόνες 1 & 2: Προβολή self-signed πιστοποιητικό από Windows OS (αριστερά) και Linux OS (δεξιά).

```
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ touch ca.cnf
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ ls
ca.cnf  cacnf  certs  my-safe-directory
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl genrsa -out my-safe-directory/ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ chmod 400 my-safe-directory/ca.key
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl req -new -x509 -config ca.cnf -key my-safe-di
rectory/ca.key -out certs/ca.crt -days 365 -batch
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl genrsa -out my-safe-directory/ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ chmod 400 my-safe-directory/ca.key
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl req -new -x509 -config ca.cnf -key my-safe-di
rectory/ca.key -out certs/ca.crt -days 365 -batch
problems making Certificate Request
139791690835264:error:0D07A098:asn1 encoding routines:ASN1_mbstring_ncopy:string too short:crypto/asn1/a_mbstr.c:100:minsize=1
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl req -new -x509 -config ca.cnf -key my-safe-di
rectory/ca.key -out certs/ca.crt -days 365 -batch
```

Εικόνα 3: Διαδικασία δημιουργίας self-signed πιστοποιητικού σε Linux.

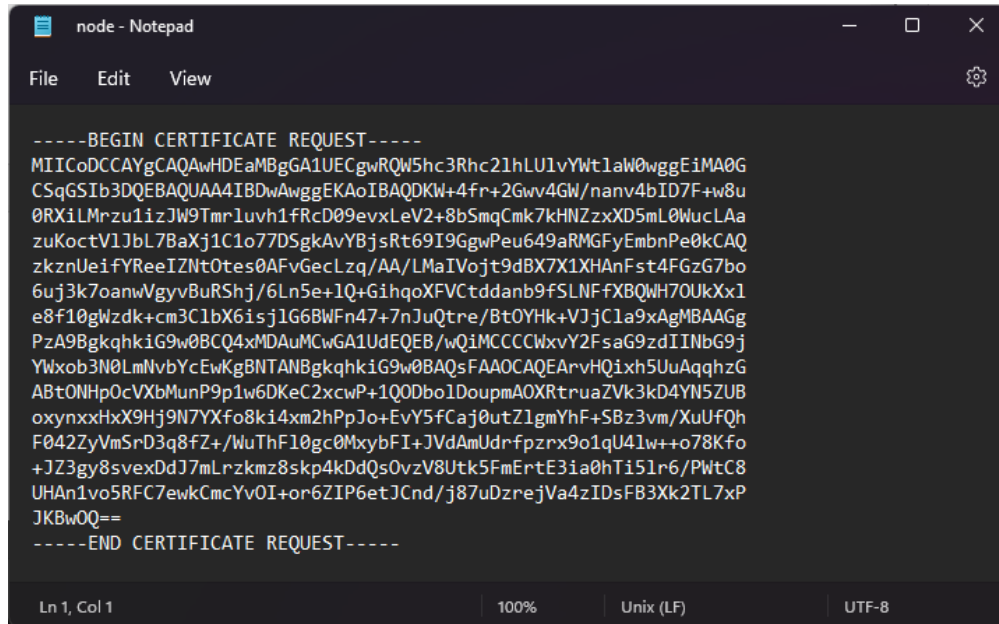
2. Δημιουργία και Πιστοποίηση Κλειδιών για Server

Δημιουργήθηκε το παρακάτω ζεύγος κλειδιών για τον web server Kestrel (Εικόνες 4 & 5).



Εικόνες 4 & 5: Προβολή ζεύγους κλειδιών για τον Kestrel Server από Windows OS (αριστερά) και Linux OS (δεξιά).

Στη συνέχεια, δημιουργήθηκε ένα αίτημα certificate signing request (csr) προς την δοκιμαστική ΑΠ ώστε να υπογράψει το πιστοποιητικό του Kestrel, τροποποιώντας κατάλληλα το αρχείο διαμόρφωσης της ΑΠ ώστε το πιστοποιητικό του server να περιλαμβάνει τα αντίστοιχα constraints (basic constraints, key usage, extended key usage) που αντιστοιχούν σε αυτόν (Εικόνα 6).



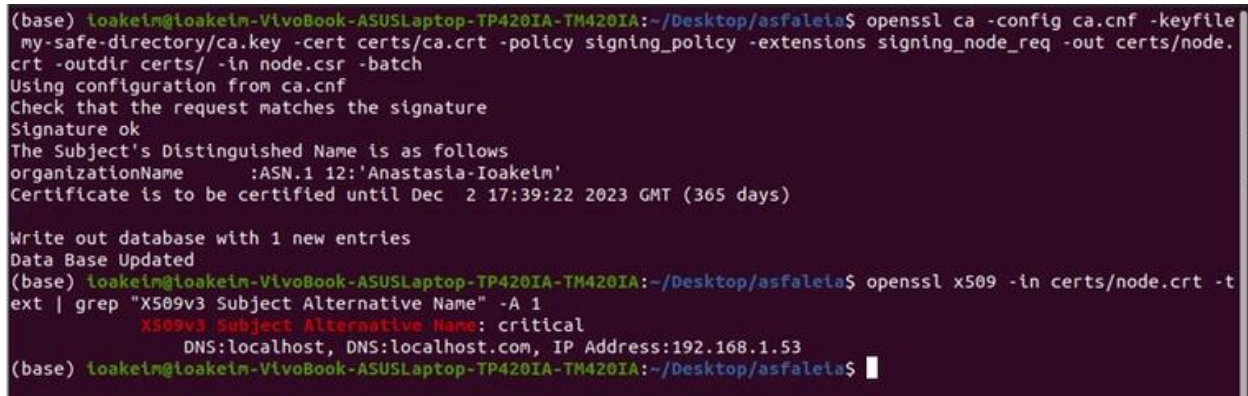
```
node - Notepad
File Edit View

-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwHDEaMBGGA1UECgwRQW5hc3RhczI1hLU1vYWtlaW0wggiEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDKW+4fr+2Gwv4GW/nanv4bID7F+w8u
0RXiLMrzu1izJW9Tmr1uvh1fRcD09evxLeV2+8bSmqCmk7kHNZzxXD5mL0WucLAA
zuKoctV1JbL7BaXj1C1o77DSgkAvYBjsRt69I9GgwPew649aRMGFyEmbnPe0kCAQ
zkznUeifYReeIZNt0tes0AFvGecLzq/AA/LMaIVojt9dBX7X1XHAnFst4FGzG7bo
6uj3k7oanwVgyvBuRShj/6Ln5e+1Q+GihqoXFVctddanb9fSLNFfXBQW70UkXx1
e8f10gWzdk+cm3C1bX6isjlG6BWFN47+7nJuQtire/BtOYHk+VJjC1a9xAgMBAAGg
PzA9BgkqhkiG9w0BCQ4xMDAuMCwGA1UdEQEB/wQIMCCCCWxvY2FsaG9zdIINbG9j
YXxob3N0LmNvbYcEwKgBNTANBgkqhkiG9w0BAQsFAAOCAGEArvHQixh5UuAqghzG
ABtONhp0cVXBmUnP9p1w6DKEc2xcwP+1Q0Dbo1DoupmaOXRtruaZVk3kD4YN5ZUB
oxynxxHxX9Hj9N7YXfo8ki4xm2hPpJo+EvY5fCaj0utZlgmYhF+SBz3vm/XuUfQh
F042ZyVmSrD3q8fZ+/WuThF10gc0MxybFI+JVdAmUdrfpzrx9o1qU41w++o78Kfo
+JZ3gy8svexDdJ7mLrzkmz8skp4kDdQs0vzV8Utk5FmErtE3ia0hTi51r6/PWtC8
UHAN1vo5RfC7ewkCmcYvOI+or6ZIP6etJCnd/j87uDzrejVa4zID5FB3Xk2TL7xP
JKBwOQ==
-----END CERTIFICATE REQUEST-----

Ln 1, Col 1 100% Unix (LF) UTF-8
```

Εικόνα 6: Certificate Signing Request προς την δοκιμαστική ΑΠ.

Η διαδικασία που ακολουθήθηκε, σε περιβάλλον Linux, φαίνεται στην Εικόνα 7.



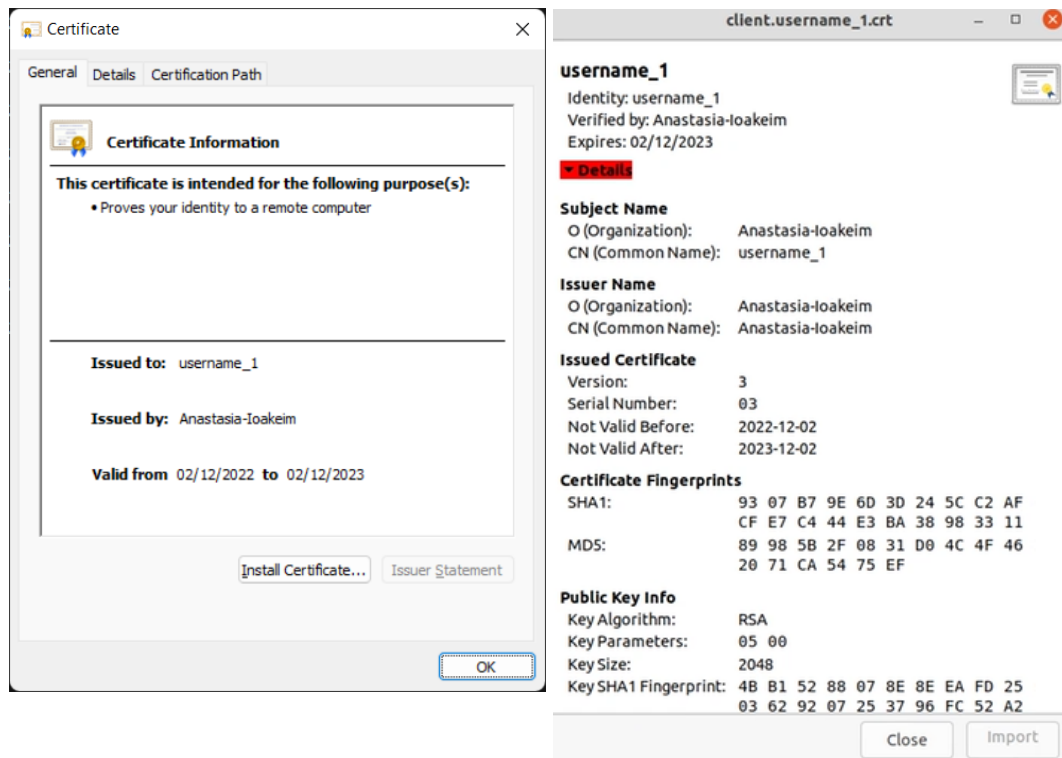
```
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl ca -config ca.cnf -keyfile
my-safe-directory/ca.key -cert certs/ca.crt -policy signing_policy -extensions signing_node_req -out certs/node.
crt -outdir certs/ -in node.csr -batch
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
organizationName      :ASN.1 12:'Anastasia-Ioakeim'
Certificate is to be certified until Dec  2 17:39:22 2023 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl x509 -in certs/node.crt -t
ext | grep "X509v3 Subject Alternative Name" -A 1
X509v3 Subject Alternative Name: critical
DNS:localhost, DNS:localhost.com, IP Address:192.168.1.53
(base) loakeim@loakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$
```

Εικόνα 7: Διαδικασία δεύτερου ερωτήματος σε Linux

3. Δημιουργία, πιστοποίηση και ανάκληση κλειδών

Δημιουργήθηκε το παρακάτω πιστοποιητικό για την αυθεντικοποίηση χρήστη (Εικόνες 7 & 8).



Εικόνες 8 & 9: Προβολή πιστοποιητικού αυθεντικοποίησης χρήστη από Windows OS (αριστερά) και Linux OS (δεξιά).

Η διαδικασία που ακολουθήθηκε, σε περιβάλλον Linux, φαίνεται στην Εικόνα 10.

```
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfalet$ chmod 400 certs/client.username_1.key
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfalet$ openssl req -new -config client.cnf -key certs/client.<username_1>.key -out client.username_1.csr -batch
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfalet$ openssl req -new -config client.cnf -key certs/client.username_1.key -out client.username_1.csr -batch
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfalet$ openssl ca -config ca.cnf -keyfile my-safe-directory/ca.key -cert certs/ca.crt -policy signing_policy -extensions signing_client_req -out certs/client.username_1.crt -outdir certs/ -in client.username_1.csr -batch
Using configuration from ca.cnf
check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
organizationName      :ASN.1 12:'Anastasia-Ioakeim'
commonName            :ASN.1 12:'username_1'
certificate is to be certified until Dec  2 17:49:55 2023 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfalet$
```

Εικόνα 10: Δημιουργία πιστοποιητικού αυθεντικοποίησης χρήστη σε Linux

Στη συνέχεια, η ΑΠ ανακαλεί το πιστοποιητικό αυθεντικοποίησης χρήστη και το προσθέτει στο Certificate Revocation List (Εικόνες 11, 12 & 13).

```
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl ca -config ca.cnf -keyfile my-safe-directory/ca.key -cert certs/ca.crt -gencrl -out crl/crl.pem
Using configuration from ca.cnf
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$
```

Εικόνα 11: Δημιουργία Certificate Revocation List

```
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl ca -config ca.cnf -revoke ~/Desktop/asfaleia/certs/03.pem -keyfile ~/Desktop/asfaleia/my-safe-directory/ca.key -cert ~/Desktop/asfaleia/certs/ca.crt
Using configuration from ca.cnf
Revoking Certificate 03.
Data Base Updated
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$
```

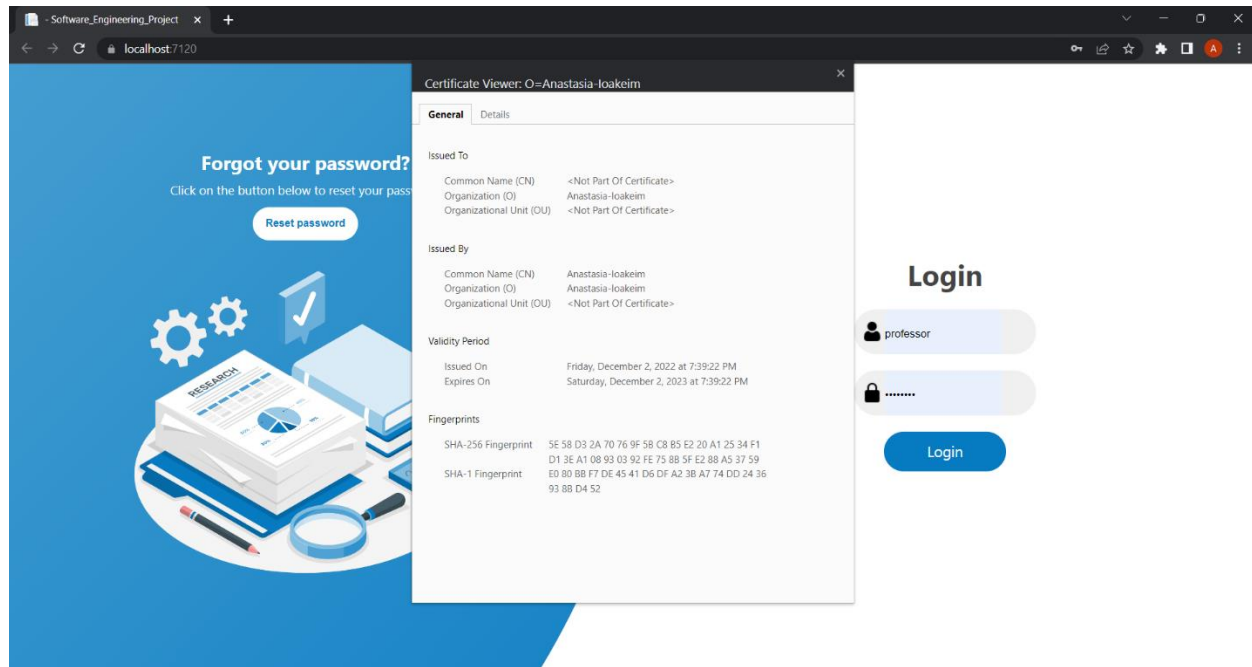
Εικόνα 12: Ανάκληση πιστοποιητικού

```
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl ca -config ca.cnf -keyfile my-safe-directory/ca.key -cert certs/ca.crt -gencrl -out crl/crl.pem
Using configuration from ca.cnf
(base) ioakeim@ioakeim-VivoBook-ASUSLaptop-TP420IA-TM420IA:~/Desktop/asfaleia$ openssl crl -in crl/crl.pem -text
Certificate Revocation List (CRL):
Version 1 (0x0)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O = Anastasia-Ioakeim, CN = Anastasia-Ioakeim
Last Update: Dec 3 14:51:32 2022 GMT
Next Update: Dec 2 14:51:32 2024 GMT
Revoked Certificates:
  Serial Number: 03
    Revocation Date: Dec 2 18:13:45 2022 GMT
    Signature Algorithm: sha256WithRSAEncryption
    86:b3:07:f6:8c:11:27:4a:96:92:54:b1:59:08:b9:89:07:f7:
    3d:b6:52:ad:a4:8c:d8:ed:ef:16:b0:33:b1:31:ba:0f:2d:9a:
    1d:d9:0a:42:f8:ed:dc:89:3c:ff:3c:2c:df:9b:e8:52:af:47:
    65:12:36:ea:ad:df:a8:49:c3:08:31:8a:ba:67:7a:da:a0:78:
    09:07:d1:3c:bd:e5:19:91:11:1e:ce:3a:27:1d:5e:69:5c:df:
    0a:f4:29:8a:69:d6:fe:53:b2:21:b8:47:69:32:18:df:34:0f:
    23:be:12:c8:93:7c:28:ff:ba:00:4d:9c:a1:55:84:af:93:03:
    0b:11:93:c3:f9:2c:1d:b7:8b:57:77:7b:c8:3f:66:f7:af:61:
    d0:a5:0a:23:34:e1:43:7e:79:6b:1a:9a:8f:1c:c1:dd:aa:93:
    b1:6d:a4:78:03:7e:b3:44:4c:82:b7:b3:48:90:17:79:98:03:
    f6:3b:bf:da:cc:37:aa:21:44:aa:89:0b:de:0c:a3:91:d8:81:
    e8:32:0b:f1:27:8f:87:90:96:0b:81:02:be:39:78:8f:53:08:
    f6:5f:ed:95:28:f6:e8:08:fb:48:ea:29:94:4a:a2:3a:76:b5:
    94:60:c8:b0:6e:0a:bf:69:01:58:83:8a:8a:a2:72:d7:42:bd:
    79:0d:cf:38
-----BEGIN X509 CRL-----
MIIBkzB9MA0GCSCqGSIb3DQEBCwUAMGxGjAYBgNVBAoMEUFuYXN0YXNpYS1Jb2Fr
ZWltMR0wGAYDVQQDBFBmFzdGFzaWtSW9ha2VpbRcNMjIyMTQ1MTMyWWhcN
MjQxMjAyMTQ1MTMyWjAUMBIGAQQHxDTIyMTIwMjE4MTA0NDVvODQyK0ZlIhvcNAQEL
BQADggEBAIazB/aME5dKlpJUsVkiUyKH9z22Uq2kjNjt7xawM7Exug8tnh3ZCkL4
7dyJPP8BLN+b6FKvR2USNuqt36hJwmgxlrpnetqgeAKH0Ty95RMER700lCdXmLc
3wR0KYpp1VSTsIG4R2kyGN80Dyo+EsLTfcj/ugBNnKFVhK+TAWsRk8P5LB231d3
e8g/ZvevYdCLiM04UN+eWsam08cWd2qk7FtpHgDfrNETIK3s0iQF3mYA/Y7v9rM
N6ohRKqJC94Mo5HYgegyC/Enj4eQLguBAr4SeI9TCPZf7ZUo9ugI+0jqZKRkojp2
tZRgyLBuCr9pAViDloqlctdCvXkNzzg=
-----END X509 CRL-----
```

Εικόνα 13: Προσθήκη σε CRL

4. Εισαγωγή Πιστοποιητικού στον Server

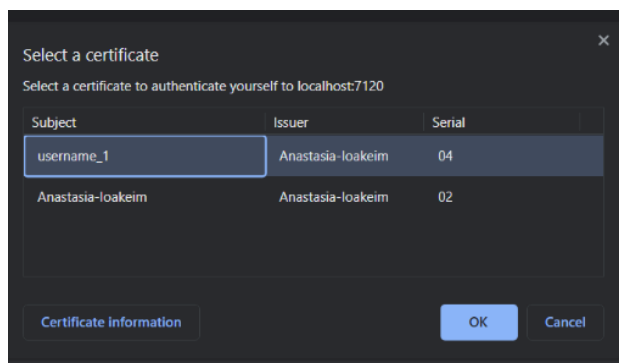
Η εισαγωγή του πιστοποιητικού στον Kestrel Server (Εικόνα 14) έγινε τροποποιώντας κατάλληλα το αρχείο appsettings.json της διαδικτυακής εφαρμογής.



Εικόνα 14: Πιστοποιητικό στον Kestrel Server

5. Διαμόρφωση του Server για διπλή αυθεντικοποίηση

Η εισαγωγή του client πιστοποιητικού (Εικόνα 15), ώστε να επιτευχθεί η διπλή αυθεντικοποίηση, έγινε τροποποιώντας κατάλληλα το αρχείο Program.cs της διαδικτυακής εφαρμογής.



Εικόνα 15: Αυθεντικοποίηση χρήστη στον Kestrel Server