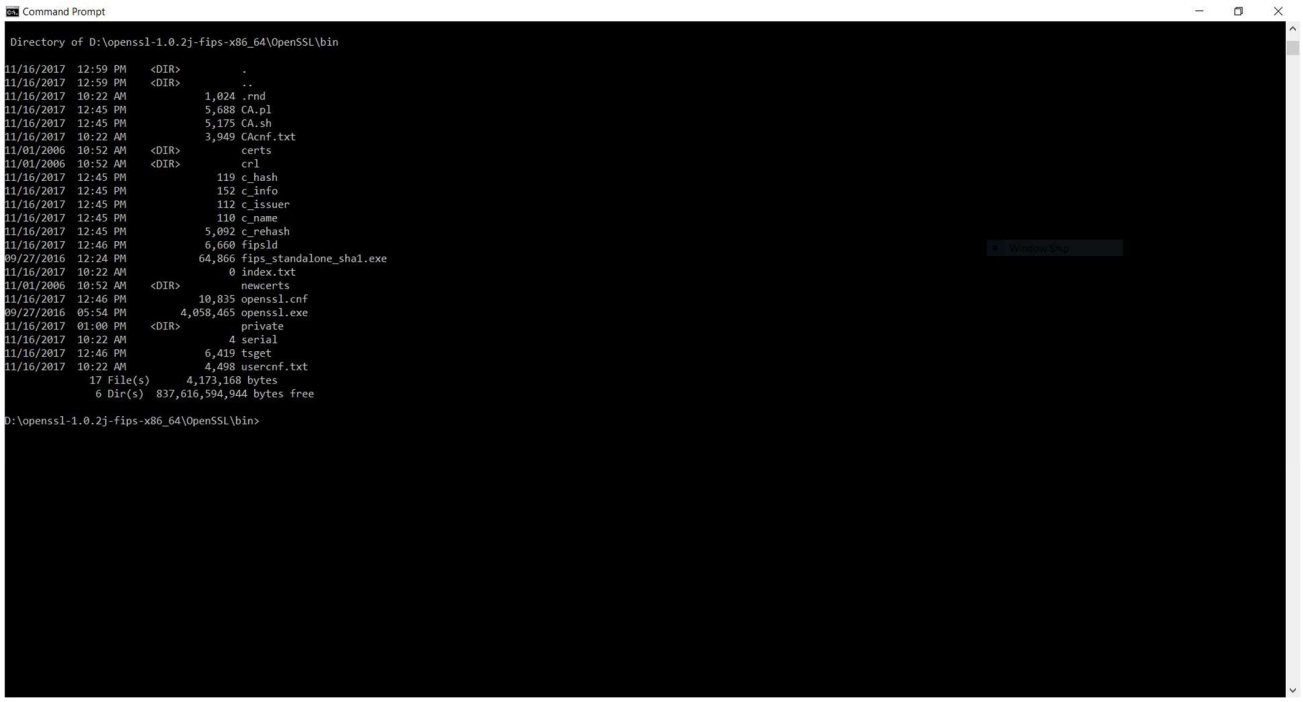
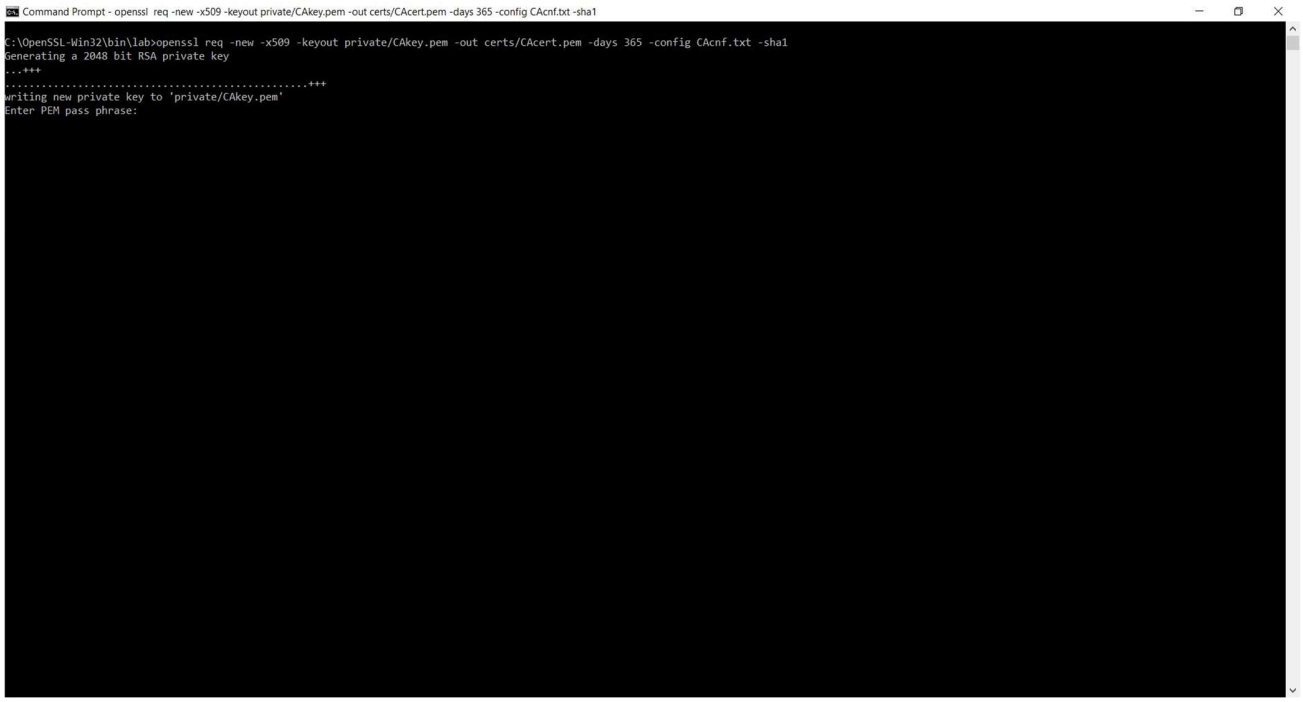
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

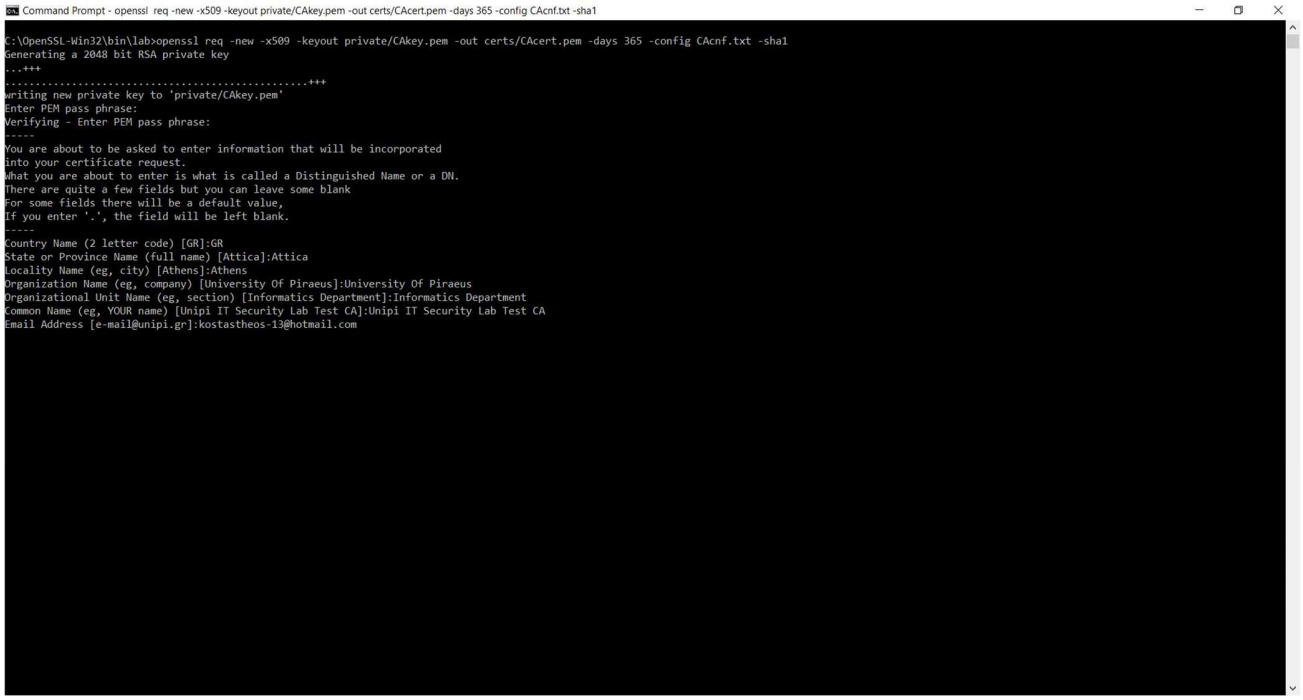
Εργασία Μαθήματος ***Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση *<<αριθμός άσκησης>>*	***3η Άσκηση-Διαχείριση πιστοποιητικών με το Openssl***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	29-10-2018

1) Δημιουργία ΑΠ: Δημιουργήστε μία δοκιμαστική ΑΠ. Η ΑΠ θα έχει αυτο-υπογεγραμμένο πιστοποιητικό (όπως στο εργαστηριακό παράδειγμα)

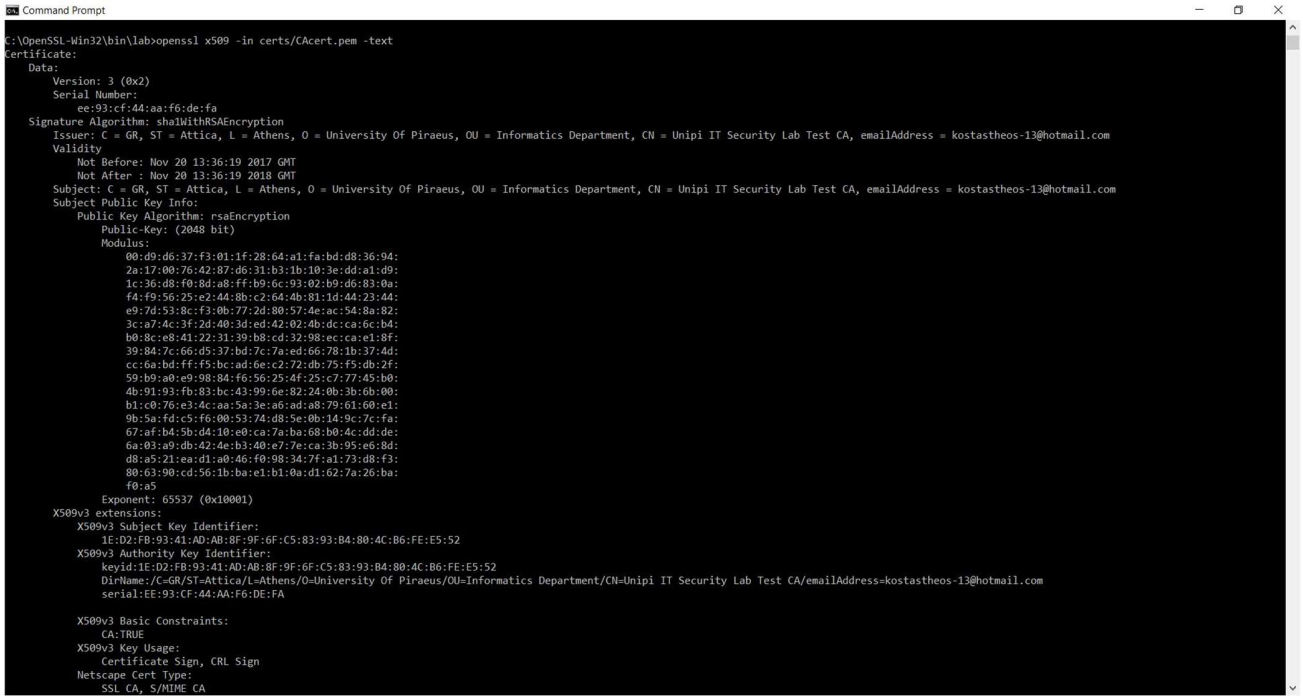


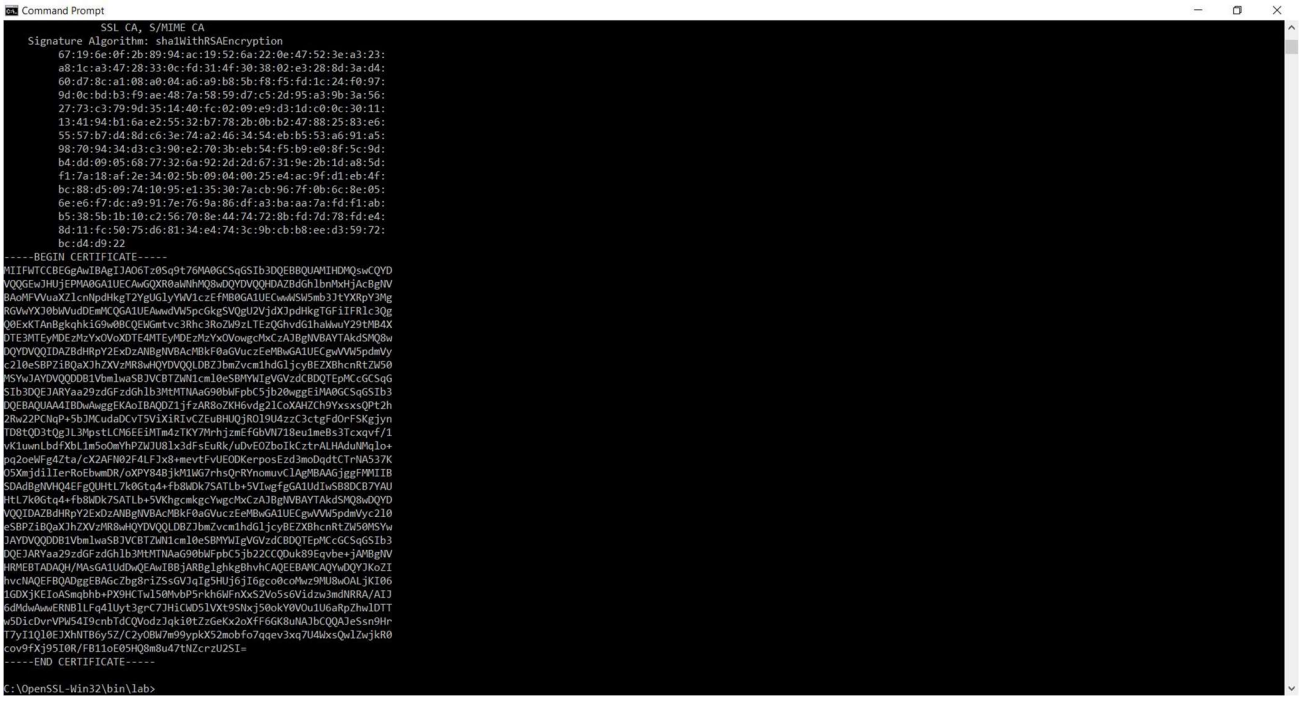

Command Prompt - openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
C:\OpenSSL-Win32\bin\lab>openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
Generating a 2048 bit RSA private key
...+++
.....+++
writing new private key to 'private/CAkey.pem'
Enter PEM pass phrase:

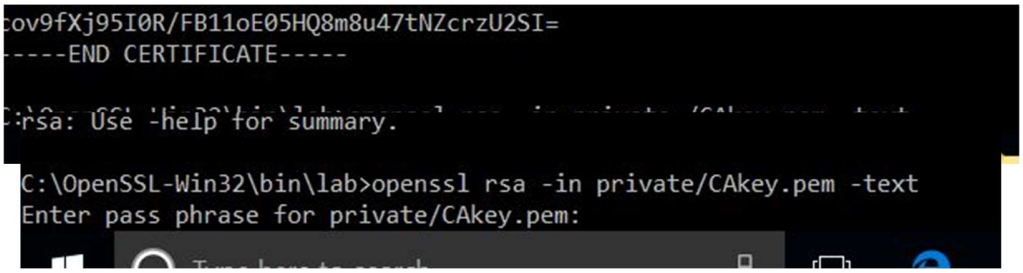

Command Prompt - openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
C:\OpenSSL-Win32\bin\lab>openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
Generating a 2048 bit RSA private key
...+++
.....+++
writing new private key to 'private/CAkey.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) [GR]:GR
State or Province Name (full name) [Attica]:Attica
Locality Name (eg, city) [Athens]:Athens
Organization Name (eg, company) [University Of Piraeus]:University Of Piraeus
Organizational Unit Name (eg, section) [Informatics Department]:Informatics Department
Common Name (eg, YOUR name) [Unipi IT Security Lab Test CA]:Unipi IT Security Lab Test CA
Email Address [e-mail@unipi.gr]:kostastheos-13@hotmail.com


Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl x509 -in certs/CAcert.pem -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ee:93:cf:44:aa:f6:de:fa
Signature Algorithm: sha1WithRSAEncryption
Issuer: C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
Validity
Not Before: Nov 20 13:36:19 2017 GMT
Not After : Nov 20 13:36:19 2018 GMT
Subject: C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d9:d6:37:f3:01:1f:28:64:a1:fa:bd:d8:36:94:
2a:17:00:76:42:87:d6:31:b3:1b:10:3e:dd:a1:d9:
1c:36:d8:f0:8d:a8:ff:b9:6c:93:02:b9:d6:83:0a:
f4:f9:56:25:e2:44:8b:c2:64:4b:81:1d:44:23:44:
e9:7d:53:8c:f3:0b:77:2d:80:57:4e:ac:54:8a:82:
3c:a7:4c:3f:2d:40:3d:ed:42:02:4b:dc:ca:6c:b4:
b0:8c:e8:41:22:31:39:b8:cd:32:98:ec:ca:e1:8f:
39:84:7c:66:d5:37:bd:7c:7a:ed:66:78:1b:37:4d:
cc:6a:bd:ff:f5:bc:ad:6e:c2:72:db:75:f5:db:2f:
59:b9:a0:e9:98:84:f6:56:25:4f:25:c7:77:45:b0:
4b:91:93:fb:83:bc:43:99:6e:82:24:0b:3b:6b:00:
b1:c0:76:e3:4c:aa:5a:3e:a6:ad:a8:79:61:60:e1:
9b:5a:fd:c5:f6:00:53:74:d8:5e:0b:14:9c:7c:fa:
67:af:b4:5b:d4:10:e0:ca:7a:ba:68:b0:4c:dd:de:
6a:03:a9:db:42:4e:b3:40:e7:7e:ca:3b:95:e6:8d:
d8:a5:21:ea:d1:a0:46:f0:98:34:7f:a1:73:d8:f3:
80:63:90:cd:56:1b:ba:e1:b1:0a:d1:62:7a:26:ba:
f0:a5
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
1E:D2:FB:93:41:AD:AB:8F:9F:6F:C5:83:93:B4:80:4C:B6:FE:E5:52
X509v3 Authority Key Identifier:
keyid:1E:D2:FB:93:41:AD:AB:8F:9F:6F:C5:83:93:B4:80:4C:B6:FE:E5:52
DirName:/C=GR/ST=Attica/L=Athens/O=University Of Piraeus/OU=Informatics Department/CN=Unipi IT Security Lab Test CA/emailAddress=kostastheos-13@hotmail.com
serial:EE:93:CF:44:AA:F6:DE:FA
X509v3 Basic Constraints:
CA:TRUE
X509v3 Key Usage:
Certificate Sign, CRL Sign
Netscape Cert Type:
SSL CA, S/MIME CA


Command Prompt
SSL CA, S/MIME CA
Signature Algorithm: sha1WithRSAEncryption
67:19:6e:0f:2b:89:94:ac:19:52:6a:22:0e:47:52:3e:a3:23:
a8:1c:a3:47:28:33:0c:fd:31:4f:30:38:02:e3:28:8d:3a:d4:
60:d7:8c:a1:08:a0:04:a6:a9:b8:5b:f8:f5:fd:1c:24:f0:97:
9d:0c:bd:b3:f9:ae:48:7a:58:59:d7:c5:2d:95:a3:9b:3a:56:
27:73:c3:79:9d:35:14:40:fc:02:09:e9:d3:1d:c0:0c:30:11:
13:41:94:b1:6a:e2:55:32:b7:78:2b:0b:b2:47:88:25:83:e6:
55:57:b7:d4:8d:c6:3e:74:a2:46:34:54:eb:b5:53:a6:91:a5:
98:70:94:34:d3:c3:90:e2:70:3b:eb:54:f5:b9:e0:8f:5c:9d:
b4:dd:09:05:68:77:32:6a:92:2d:2d:67:31:9e:2b:1d:a8:5d:
f1:7a:18:af:2e:34:02:5b:09:04:00:25:e4:ac:9f:d1:eb:4f:
bc:88:d5:09:74:10:95:e1:35:30:7a:cb:96:7f:0b:6c:8e:05:
6e:e6:f7:dc:a9:91:7e:76:9a:86:df:a3:ba:aa:7a:fd:f1:ab:
b5:38:5b:1b:10:c2:56:70:8e:44:74:72:8b:fd:7d:78:fd:e4:
8d:11:fc:50:75:d6:81:34:e4:74:3c:9b:cb:b8:ee:d3:59:72:
bc:d4:d9:22
-----BEGIN CERTIFICATE-----
MIIFWTCCBEGgAwIBAgIJAO6Tz0Sq9t76MA0GCSqGSIb3DQEBBQUAMIHDMQswCQYD
VQQGEwJHUjEPMA0GA1UECAwGQXR0aWNhMQ8wDQYDVQQHDAZBdGh1bnMxHjAcBgNV
BAoMFVVuaXZlcnNpdHkgT2YgUGlyYWV1czEfMB0GA1UECwwWSW5mb3JtYXRpY3Mg
RGVwYXJ0bWVudDEmMCQGA1UEAwwdVW5pcGkgSVQgU2VjdXJpdHkgTGFiIFRlc3Qg
Q0ExKTAnBgkqhkiG9w0BCQEWGmtvc3Rhc3Rob3ZW9zLTEzQGhvdG1haWwuY29tMB4X
DTE3MTEyMDEzMzYxOVoXDTE4MTEyMDEzMzYxOVowgcMxCzAJBgNVBAYTAkdSMQ8w
DQYDVQQIDAZBdHRpY2ExDzANBgNVBAcMBkF0aGVuczEeMBwGA1UECgwVVW5pdmVy
c2l0eSBPZiBQaXJhZXVzMR8wHQYDVQQLDBZJbmZvcm1hdGljcyBEZXBhcnRtZW50
MSYwJAYDVQQDDB1VbmlwaSBJVCBTZWN1cml0eSBMYWIgVGVzdCBDQTEpMCcGCSqG
SIb3DQEJARYaa29zdGFzdGhlb3MtMTNAaG90bWFpbC5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDZ1jfzAR8oZKH6vdg2lCoXAHZCh9YxsxsQPt2h
ZRw22PCNqP+5bJMCudaDCvT5ViXiRIvCZEuBHUQjRO19U4zzC3ctgFdOrFSKgjyn
TD8tQD3tQgJL3MpstLCM6EEiMTm4zTKY2MrhjzmEfGbVN718eu1meBs3Tcxqvf/1
yK1uwnLbdfXb1m5oOmYhPZbUJU8lx3dFsEuRk/uDvEOZboIkCztrALHAduNKqlo+
pq2oeWFg4Zta/cX2AFN02F4LFJx8+mevtFvUEODKerposEzd3moDqdtCTrNA537K
O5XmjdiITerRoEbwmDR/oXPY84BjkM1WG7rhsQrRYnomuvClAgMBAAGjggFMMIIB
SDAdBgNVHQ4EFgQUHtL7k0Gtq4+fb8WDk7SATLb+5VIwgfgGA1UdIwSB8DCB7YAU
HtL7k0Gtq4+fb8WDk7SATLb+5VKhgcmkgcYwgcMxCzAJBgNVBAYTAkdSMQ8wDQYD
VQQIDAZBdHRpY2ExDzANBgNVBAcMBkF0aGVuczEeMBwGA1UECgwVVW5pdmVyc2l0
eSBPZiBQaXJhZXVzMR8wHQYDVQQLDBZJbmZvcm1hdGljcyBEZXBhcnRtZW50MSYw
JAYDVQQDDB1VbmlwaSBJVCBTZWN1cml0eSBMYWIgVGVzdCBDQTEpMCcGCSqGSIb3
DQEJARYaa29zdGFzdGhlb3MtMTNAaG90bWFpbC5jb22CCQDuk89Eqvbe+jAMBgNV
HRMEBTADAQH/MAsGA1UdDwQEAwIBBjARBglghkgBhvhCAQEEBAMCAQYwDQYJKoZI
hvcNAQEFBQADggEBAGcZbg8riZssGVJqIg5HUj6jI6gco0coMwz9MU8wOALjKI06
1GDXjKEIoASmqbhb+PX9HCTwl50MvbP5rkh6WFnXxS2Vo5s6Vidzw3mdNRRA/AIJ
6dMdwAwwERNBllFq41Uyt3grC7JHiCWD5lVXt9SNxj50okY0VOu1U6aRpZhwlDTT
w5DicDvrVPW54I9cnbTdCQVodzJqki0tZzGeKx2oXfF6GK8uNAJbCQQAJeSsn9Hr
T7yI1Ql0EJXhNTB6y5Z/C2yOBW7m99ypkX52mobfo7qqev3xq7U4WxsQwlZwjkR0
cov9fXj95I0R/FB11oE05HQ8m8u47tNZcrzU2SI=
-----END CERTIFICATE-----
C:\OpenSSL-Win32\bin\lab>


cov9fXj95I0R/FB11oE05HQ8m8u47tNZcrzU2SI=
-----END CERTIFICATE-----
C:\rsa: Use -help for summary.
C:\OpenSSL-Win32\bin\lab>openssl rsa -in private/CAkey.pem -text
Enter pass phrase for private/CAkey.pem:


Command Prompt
exponent2:
7f:34:e8:59:2e:d1:3a:f8:4e:8f:17:e2:ad:71:94:
5c:9b:ef:37:f2:5b:d2:73:b6:ff:cd:a4:3d:cf:f5:
99:a1:0f:06:1e:d2:c7:e0:1d:89:38:63:30:2a:ba:
ba:a0:0d:ee:56:67:9d:e5:3b:d4:e3:7a:72:47:bb:
e3:f8:a5:53:e9:3b:b2:48:57:f7:d5:53:8c:93:96:
4d:bc:bb:f1:b7:09:5a:8d:42:0d:a6:33:15:4d:8f:
a5:e3:0e:b5:c1:e5:d6:74:b2:26:b4:94:65:b0:aa:
55:d2:1b:49:03:ac:23:59:f4:aa:d1:9f:c3:3f:26:
74:9a:3d:c9:2f:d3:bc:3d
coefficient:
22:19:ec:2d:04:79:f1:2c:45:97:40:a6:ba:59:75:
35:3e:e2:11:9d:32:55:92:38:1c:80:86:31:56:44:
90:98:93:53:1e:cd:2a:a7:c4:b7:f7:09:00:4a:1a:
6c:3b:85:3e:a8:d1:33:41:62:c9:d2:5a:52:96:8c:
dd:7c:4c:1f:e6:4a:36:26:e6:4d:cc:d1:e8:0a:86:
3e:21:f0:4d:18:37:d9:5f:a5:8d:63:91:42:b4:61:
ca:dd:1b:34:d1:5a:36:0b:7b:da:af:7e:05:e3:23:
fc:d4:c2:ac:b5:e9:e2:cc:10:8d:13:38:58:38:47:
f2:f6:db:83:5b:9d:60:04
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA2dY38wEfKGSh+r3YNpQqFwB2QofWbMbED7dodkcNtjwjaj/
uWyTArnWgwr0+VYl4kSLwmRLgR1EI0TpfVOM8wt3LYBXTqxUioI8p0w/LUA97UIC
S9zKbLSwjOh8IjE5uM0ymOzK4Y85hHxm1Te9fHrtZngbN03Mar3/9bytbsJy23X1
2y9ZuaDpmIT2ViVPJcd3RbBLkZP7g7xDmW6CJAs7awCxwHbjTKpaPqatqHlhYOGb
vWv3F9gBTdNheCx5cfPpnr7Rb1BDgynq6aLBM3d5qA6nbQk6zQOd+yjuV5o3YpSHq
0aBG8Jg0f6FzZPOAY5DNVhu64bEK0WJ6JrrwpQIDAQABAoIBAQCT0QggTleNOlQr
6FzqFDpHZ3nYBYLUMLwhlvcf10ps8WKyTcZRVZqgU+h6/ZlkBBAq7OaFXzdZArn0
0NM7xtEzL0mMp7UW3ptzbZKo13VbSGd9MriKL+VwRGA1DXj9MbgAbcVyveOhkWWv
QBcrgepjqKqlSMT3DySyHgGtB34MVEfM3CkjlBGYhy+fZxprRBweVHTcx0e4Pydg
/Jgz2ih58Xu+yjMju6F47+V+z10Y3dGIlyMrqz6bwP8N6FT0lW5IX99ISwiuMTxm
HjUby0nlcVUIDTnduH0KMaw9AN0fs5U9b5d1gcIVPY8VqYyU8siCkxUhzdUCRKDW
3wAPu0n1AoGBAO1EKBtvejIbMaFQPJxRcR9ehM7dPRvvhBKHWkjWaaU7Qz0ZwCsa
AZ2OvPRmk9bwtUYGeIiWcobQS02bE3JvQ4yMuH/CEp1PXwHDxkGsiNIGgYqtxN98
8GzISUdm+Y6j9AbWiGt0wuSlDAAC4icb84i54xD9dTkzjXPNUCoFE1MHAoGBAOsJ
VggbNmN3ZpVUnWCG5CRvdrmOMeRtIxZdMOLxv6lS/XBqpnsXaK0HUkR+AduADfYS
QnWtlxMmYI1cU2bZ8epsk0J45IgvxkZZQZ2MVQnLOErgm9u95Oq2opa/PFQhSJhG
nn0ynbrzr/aBUHegpwgc7WYzNEZCrACj4V2IxpfzAoGBAM/qiBLyr2w1NFqeC18Y
Zz8L/umgKirOyzfJcK6fZdirhBKI/ENI+N1u9dpeAXO7X77LcNiQri/BXBvXp0UC
h3kk35DlKpa7tQ/A1X07inJfXqF+ASWvQKizIrP1Yv9CYVeUq9suaJMgptFjtXZ8
If9QldCPqyfDK1OtOXB5HiQFAoGAfzToWS7ROvhOjxfirXGUXJvvN/Jb0nO2/82k
Pc/1maEPBh7Sx+AdiThjMCq6uqAN7lZnneU71ON6cke74/ilU+k7skhX99VTjJOW
Tby78bcJWo1CDaYzFU2PpeMOtcHl1nSyJrSUZbCqVdIbSQOsI1n0qtGfwz8mdJo9
yS/TvD0CgYAiGewtBHnxLEWXQKa6WXU1PuIRnTJVkjgcgIYxVkSQmJNTHs0qp8S3
9wkAShpsO4U+qNEzQWLJ0lpSlozdfEwf5ko2JuZNzNHoCoY+IfBNGDfZX6WNY5FC
tGHK3Rs00Vo2C3var34F4yP81MKstenizBCNEzhYOEfy9tuDW51gBA==
-----END RSA PRIVATE KEY-----
C:\OpenSSL-Win32\bin\lab>

2)Δημιουργία και πιστοποίηση κλειδιών για server:Δημιουργήστε ένα ζεύγος κλειδιών για έναν web server. Στη συνέχεια φτιάξτε ένα έτοιμα certificate signing request (csr) προς την δοκιμαστική ΑΠ ώστε να υπογράψει το πιστοποιητικό του server, αντίστοιχα με το εργαστηριακό παράδειγμα. Όμως θα πρέπει να τροποποιήσετε κατάλληλα το αρχείο διαμόρφωσης της ΑΠ ώστε το πιστοποιητικό του server να περιλαμβάνει τα αντίστοιχα constraints (key usage και extended key usage) που αντιστοιχούν σε έναν server, όπως φαίνεται στο[1].

Administrator: Command Prompt

```
C:\OpenSSL-Win32\bin\lab>openssl req -new -config CAcnf.txt -nodes -keyout private/serverKey.pem -out req/server.csr -days 365 -md5
```

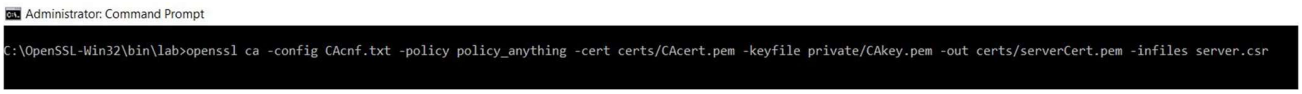
Administrator: Command Prompt

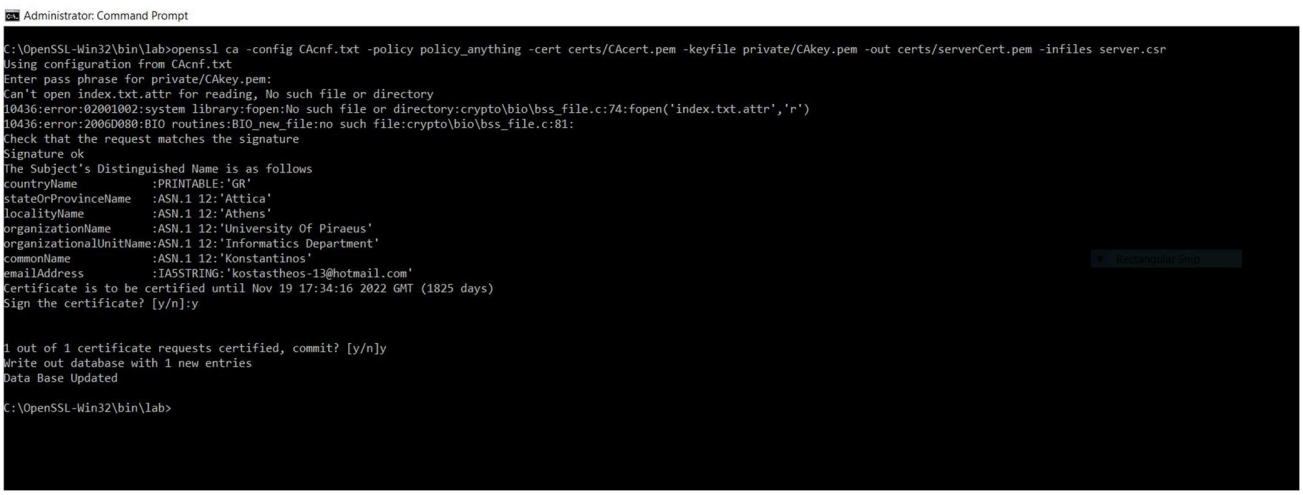
```
C:\OpenSSL-Win32\bin\lab>openssl req -new -config CAcnf.txt -nodes -keyout private/serverKey.pem -out server.csr -days 365 -md5
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'private/serverKey.pem'
-----
You are about to be asked to enter information that will 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) [GR]:GR
State or Province Name (full name) [Attica]:Attica
Locality Name (eg, city) [Athens]:Athens
Organization Name (eg, company) [University Of Piraeus]:University Of Piraeus
Organizational Unit Name (eg, section) [Informatics Department]:Informatics Department
Common Name (eg, YOUR name) [Unipi IT Security Lab Test CA]:Konstantinos
Email Address [e-mail@unipi.gr]:kostastheos-13@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pappoulis13

C:\OpenSSL-Win32\bin\lab>
```

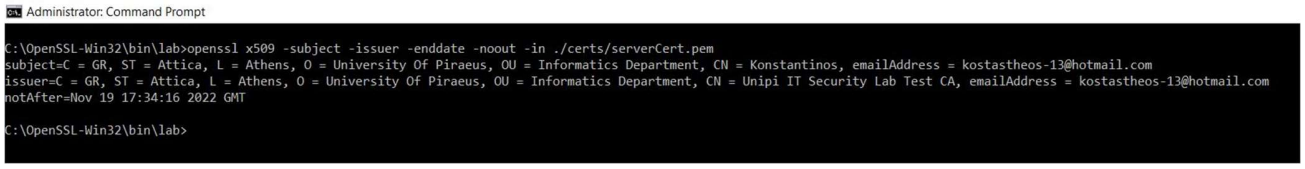
Administrator: Command Prompt

```
C:\OpenSSL-Win32\bin\lab>openssl rsa -in private/serverKey.pem -text
```

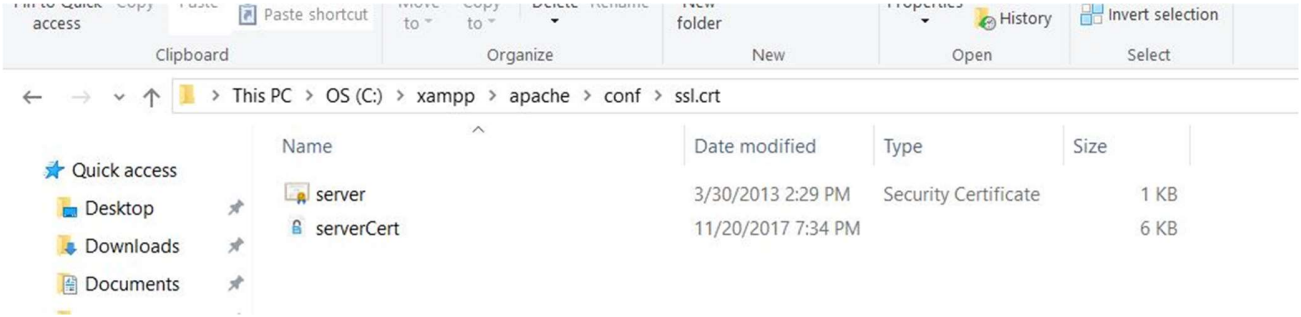
Δημιουργία έμπιστης αρχής πιστοποίησης (CA)

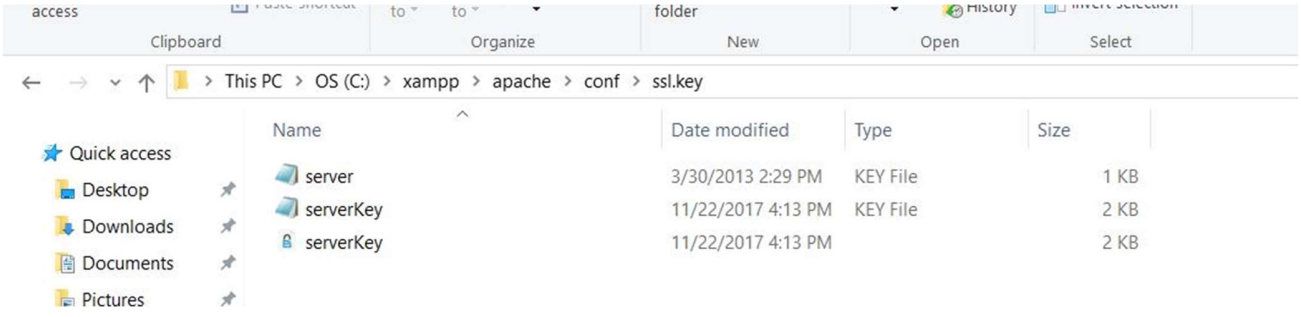

Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl ca -config CAcnf.txt -policy policy_anything -cert certs/CAcert.pem -keyfile private/CAkey.pem -out certs/serverCert.pem -infiles server.csr

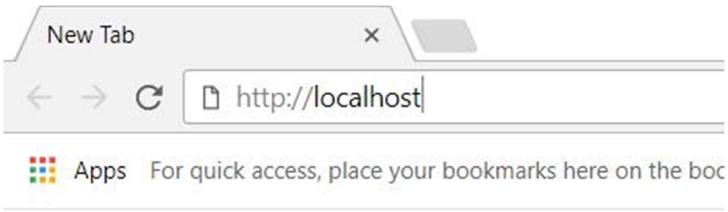

Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl ca -config CAcnf.txt -policy policy_anything -cert certs/CAcert.pem -keyfile private/CAkey.pem -out certs/serverCert.pem -infiles server.csr
Using configuration from CAcnf.txt
Enter pass phrase for private/CAkey.pem:
Can't open index.txt.attr for reading, No such file or directory
10436:error:02001002:system library:fopen:No such file or directory:crypto\bio\bss_file.c:74:fopen('index.txt.attr','r')
10436:error:2006D080:BIO routines:BIO_new_file:no such file:crypto\bio\bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'GR'
stateOrProvinceName :ASN.1 12:'Attica'
localityName :ASN.1 12:'Athens'
organizationName :ASN.1 12:'University Of Piraeus'
organizationalUnitName:ASN.1 12:'Informatics Department'
commonName :ASN.1 12:'Konstantinos'
emailAddress :IA5STRING:'kostastheos-13@hotmail.com'
Certificate is to be certified until Nov 19 17:34:16 2022 GMT (1825 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
C:\OpenSSL-Win32\bin\lab>

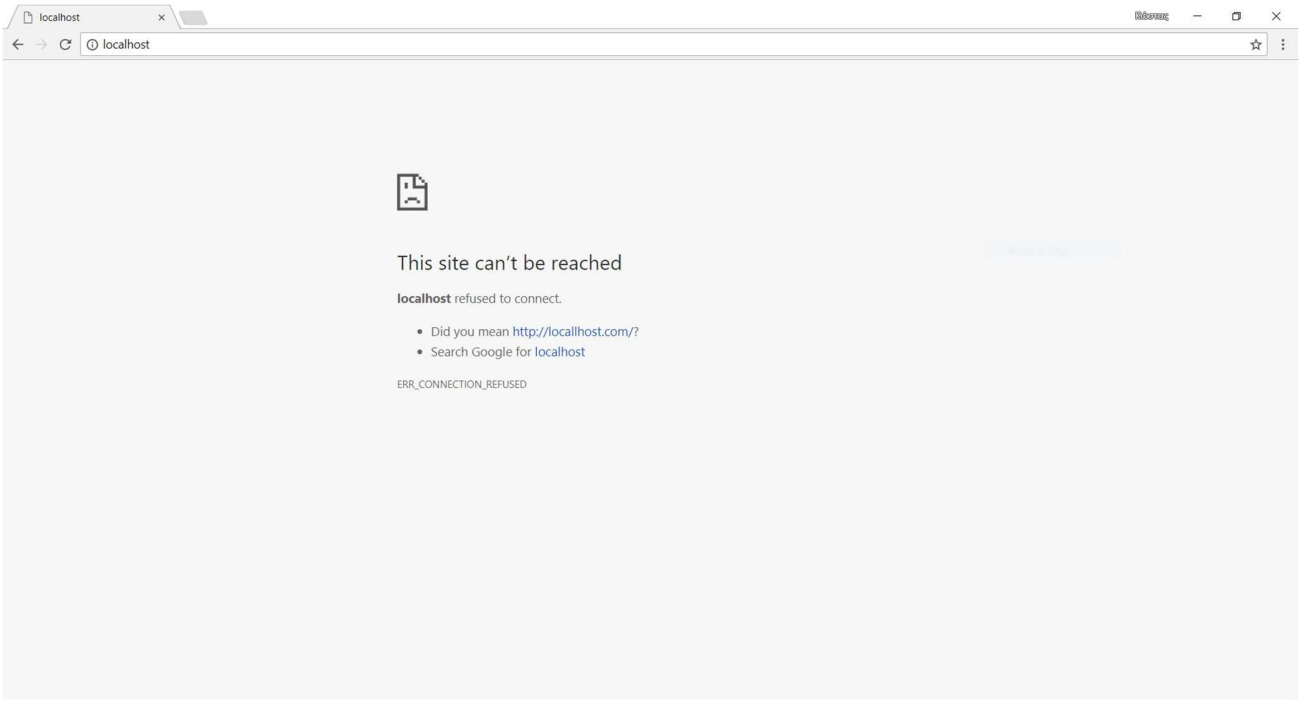

Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl x509 -subject -issuer -enddate -noout -in ./certs/serverCert.pem
subject=C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Konstantinos, emailAddress = kostastheos-13@hotmail.com
issuer=C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
notAfter=Nov 19 17:34:16 2022 GMT
C:\OpenSSL-Win32\bin\lab>

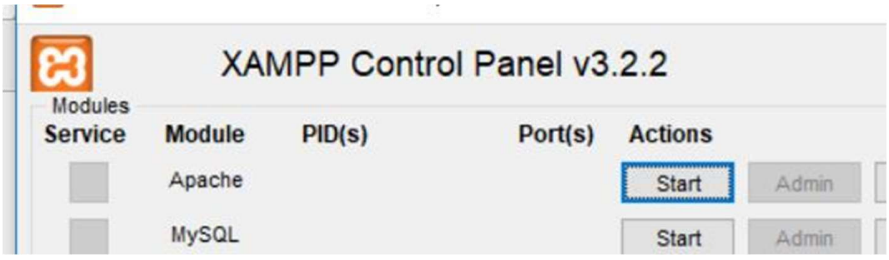
4) Εισαγωγή πιστοποιητικού στον server: Υλοποιήστε τα αντίστοιχα βήματα με το εργαστηριακό μάθημα, ώστε να εισαγάγετε το πιστοποιητικό σε έναν web server (π.χ. Apache). Τώρα ο server σας θα χρησιμοποιεί το πιστοποιητικό του για να αυθεντικοποιείται στους client (περισσότερες οδηγίες θα βρείτε στο [1] στην ενότητα One way SSL authentication)

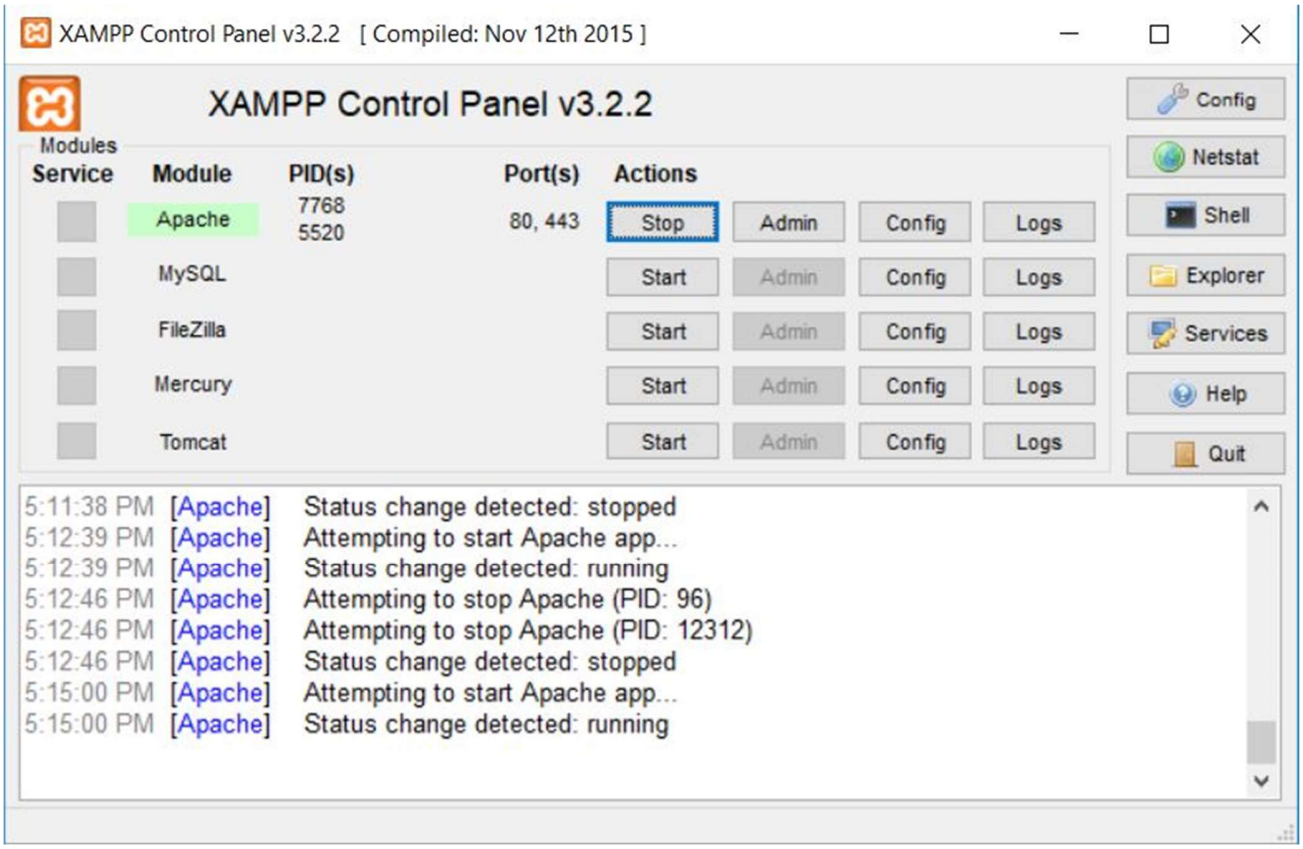


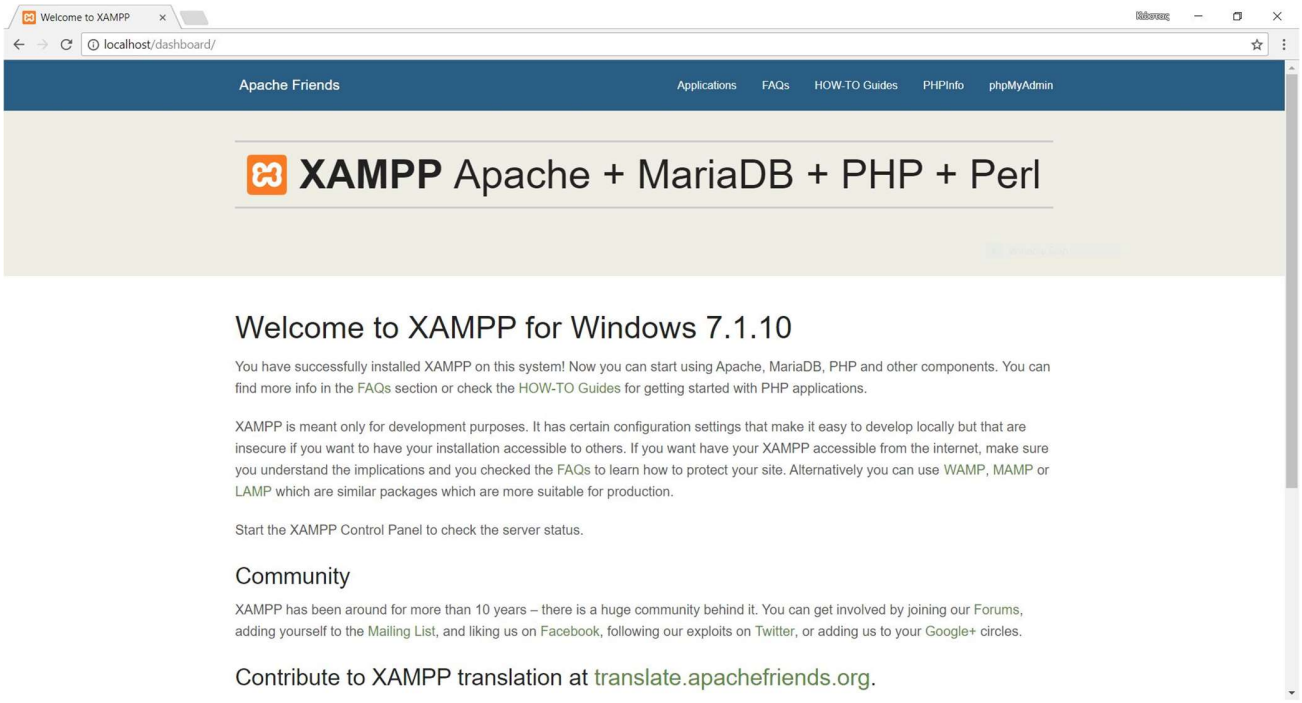


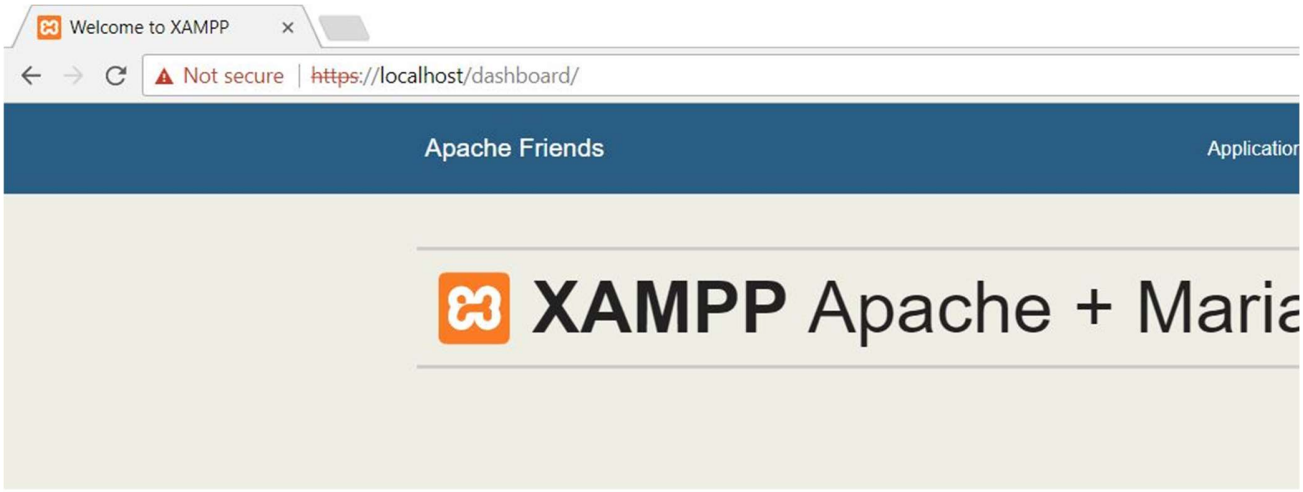



localhost
localhost
This site can't be reached
localhost refused to connect.
Did you mean http://locallhost.com/?
Search Google for localhost
ERR_CONNECTION_REFUSED


XAMPP Control Panel v3.2.2
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
Start
Admin
MySQL
Start
Admin


XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
7768
5520
80, 443
Stop
Admin
Config
Logs
MySQL
Start
Admin
Config
Logs
FileZilla
Start
Admin
Config
Logs
Mercury
Start
Admin
Config
Logs
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
5:11:38 PM [Apache] Status change detected: stopped
5:12:39 PM [Apache] Attempting to start Apache app...
5:12:39 PM [Apache] Status change detected: running
5:12:46 PM [Apache] Attempting to stop Apache (PID: 96)
5:12:46 PM [Apache] Attempting to stop Apache (PID: 12312)
5:12:46 PM [Apache] Status change detected: stopped
5:15:00 PM [Apache] Attempting to start Apache app...
5:15:00 PM [Apache] Status change detected: running


Welcome to XAMPP
localhost/dashboard/
Apache Friends
Applications
FAQs
HOW-TO Guides
PHPInfo
phpMyAdmin
XAMPP Apache + MariaDB + PHP + Perl
Welcome to XAMPP for Windows 7.1.10
You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.
XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.
Start the XAMPP Control Panel to check the server status.
Community
XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.
Contribute to XAMPP translation at translate.apachefriends.org.


Welcome to XAMPP
Not secure
https://localhost/dashboard/
Apache Friends
XAMPP Apache + Maria

5)Διαμόρφωση του server για διπλή αυθεντικοποίηση: Δημιουργείστε ένα πιστοποιητικό για client και διαμορφώστε τον server σας ώστε να απαιτεί και οι client να αυθεντικοποιούνται με τη χρήση πιστοποιητικού, και όχι με απλό password. (περισσότερες οδηγίες θα βρείτε στο [2] στην ενότητα Two-way SSL authentication). Συνδεθείτε με τον server και εξηγήστε περιληπτικά τί σημβαίνει κατά τη σύνδεση.