**OpenSSL**

Αρχικά, πάμε στο φάκελο που βρίσκεται το OpenSSL για να τρέξουμε τις αντίστοιχες εντολές 🡪 cd C:\openssl\ex\_lab2

***Σημείωση:*** *Δεν εγκαταστάθηκε το sha2, προκειμένου να κάνουμε hash με sha2. Αν ήταν εγκατεστημένο, στις εντολές αντί για ‘’sha1’’ θα βάζαμε ‘’-sha256’’.*

**E1:**

Δημιουργία αυτό-υπογεγραμμένου πιστοποιητικού για την CA και ιδιωτικού κλειδιού, με RSA,sha1, μεγέθους 4096bits, διάρκειας 4 ετών.

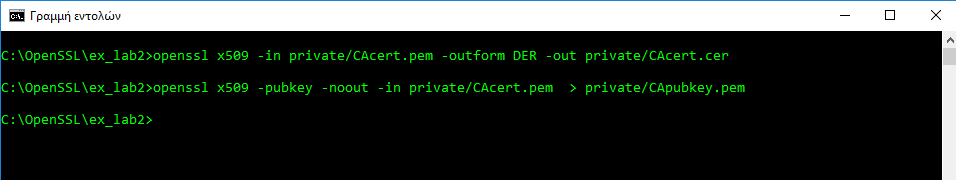
**Εκτελούμε την εντολή**: *«openssl req -x509 -newkey rsa:4096 -keyout private/CAkey.pem -out private/CAcert.pem -days 1460 -config CAcnf.txt -sha1»*



* x509: πρότυπο πιστοποιητικού
* newkey rsa:4096 : Δημιουργεί κλειδί με ζεύγος κλειδιών RSA και μέγεθος bits 4096
* -out private/… : ό,τι δημιουργείται αποθηκεύεται στον φάκελο “private”
* CAkey.pem: private key name
* CAcert.pem: certification name
* -config CAcnf.txt : παίρνει default τιμές από εκεί αν χρειαστεί.
* days 1460: 4x365 = 4 χρόνια
* sha1: hash συνάρτηση για την υπογραφή.
* Password: ca123

Με την παραπάνω εντολή, παράγεται και Public Key της CA, αλλά δεν το δημιουργούμε σε μορφή PEM. Για να το εξάγουμε, κάνουμε την εντολή:

«openssl x509 -pubkey -noout -in private/CAcert.pem > private/CApubkey.pem»



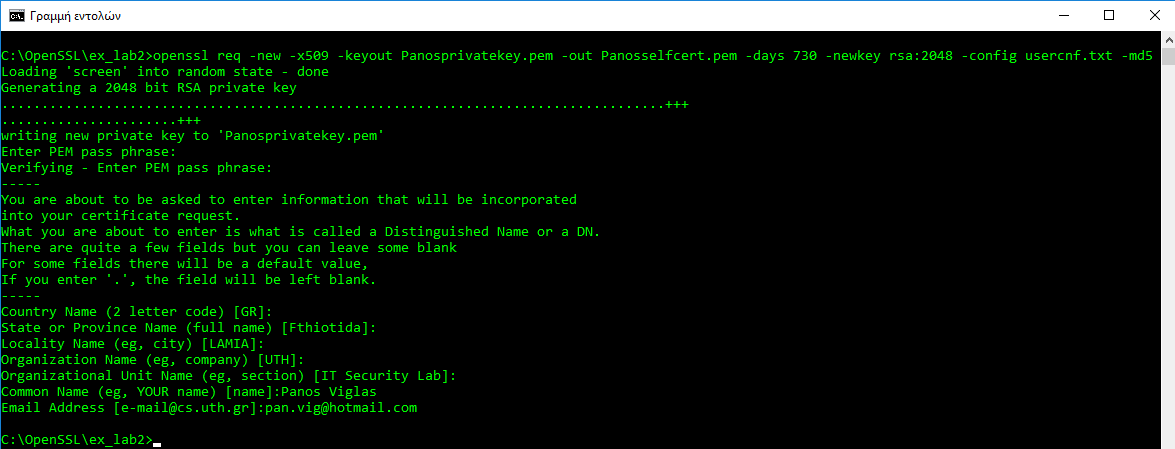
Δημιουργείται αρχείο .pem, με ονομασία «CApubkey.pem»

**E2:**

Δημιουργία Ιδιωτικού κλειδιού *(Panosprivatekey.pem)* RSA, για τον user Panos και αυτό-υπογεγραμμένου πιστοποιητικού *(Panosselfcert.pem):*

«openssl req –new –x509 –keyout Panosprivatekey.pem –out Panosselfcert.pem –days 730 –newkey rsa:2048 –config usercnf.txt –md5»

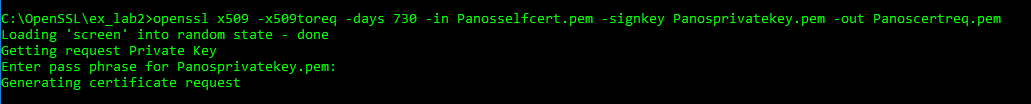
* Rsa:2048 🡪 αλγόριθμος ζεύγους κλειδιών=RSA και μέγεθος κλειδιού 2048bits
* Αλγόριθμος κατακερματισμού 🡪 -md5
* Days 730 🡪 διάρκεια 2 χρόνια



Δημιουργία αίτησης πιστοποιητικού προς υπογραφή από την CA για τον user:

«openssl x509 –x509toreq –days 730 –in Panosselfcert.pem –signkey Panosprivatekey.pem –out Panoscertreq.pem»

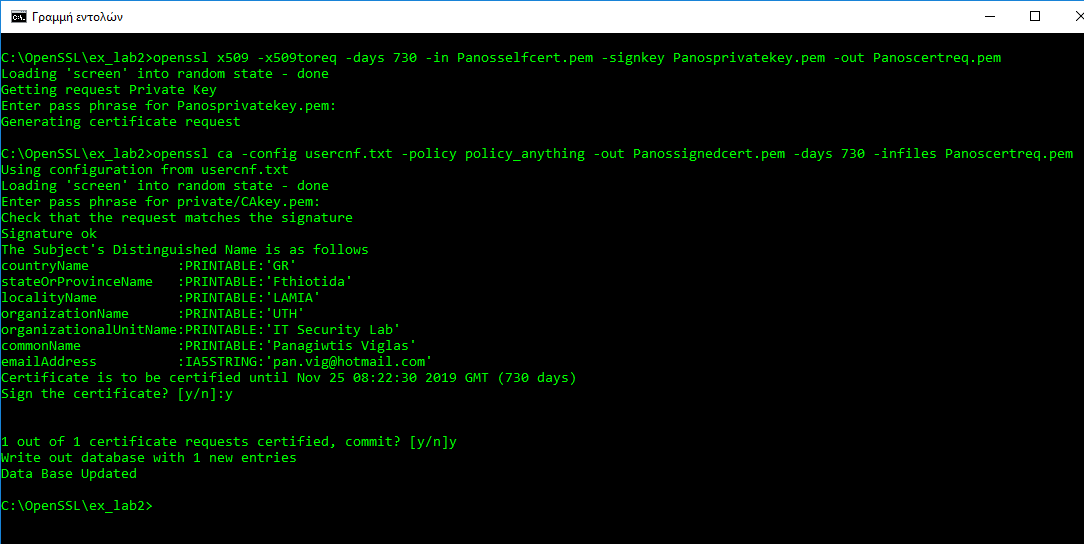
* Panoscertreq.pem 🡪 αίτηση πιστοποιητικού



Δημιουργία πιστοποιητικού χρήστη και υπογραφή του από την CA:

«openssl ca –config usercnf.txt –policy policy\_anything –out Panossignedcert.pem –days 730 –infiles Panoscertreq.pem»

* Usercnf.txt 🡪 default τιμές
* Days 730 🡪 διάρκεια 2 έτη
* Panossignedcert.pem 🡪 υπογεγραμμένο από την CA πιστοποιητικό για τον user Panos

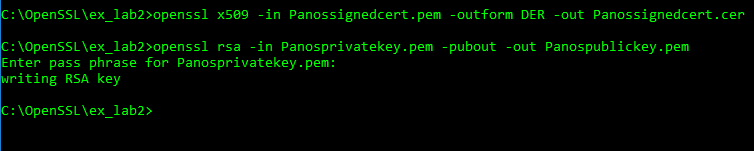


Μετατροπή του πιστοποιητικού χρήστη απο PEM σε DER:

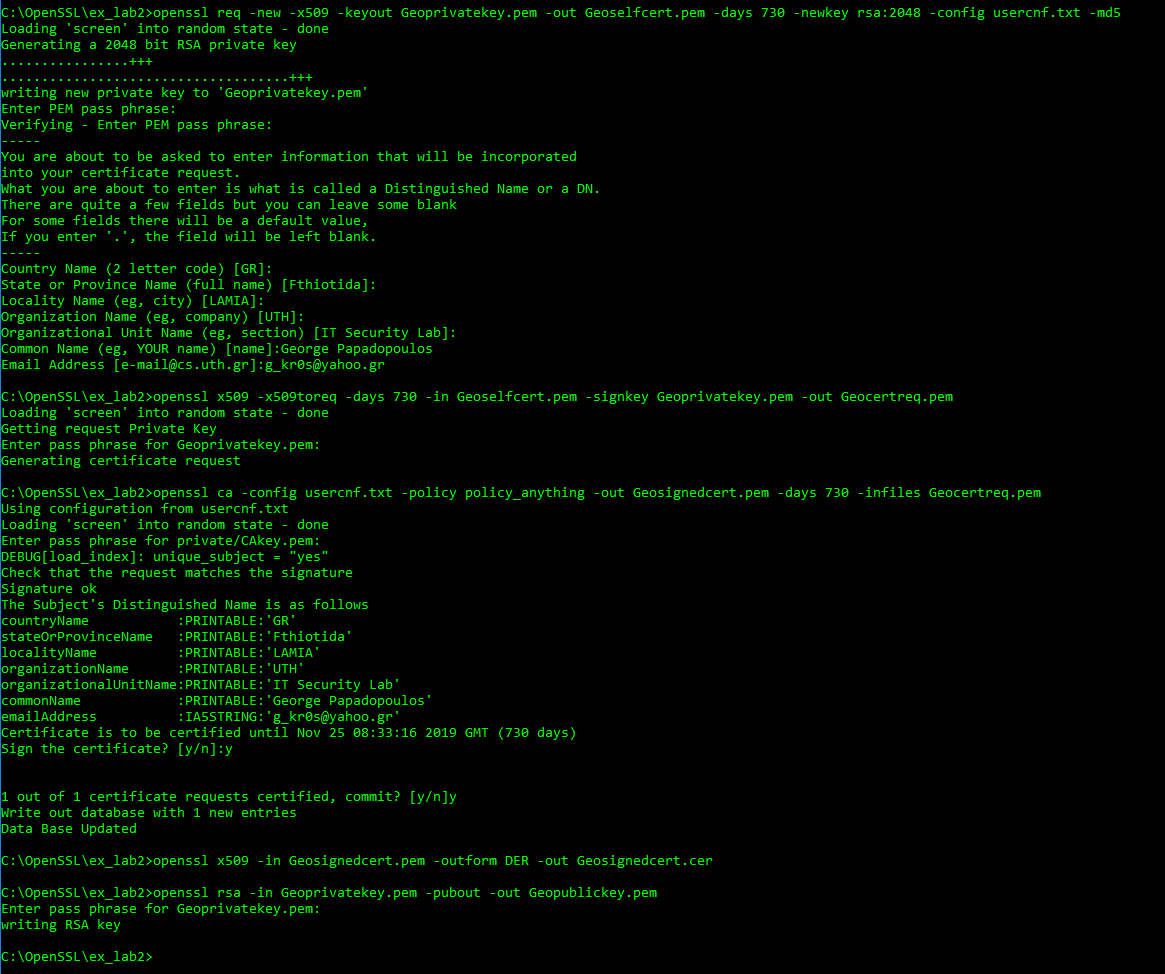
«openssl x509 –in Panossignedcert.pem –outform DER –out Panossignedcert.cer»

Λήψη δημόσιου κλειδιού χρήστη απο το ιδιωτικό:

«openssl rsa –in Panosprivatekey.pem –pubout –out Panospublickey.pem»



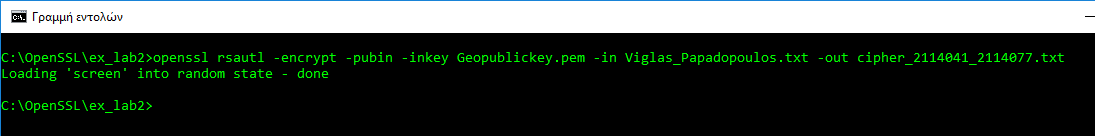
**Οι ίδιες ακριβώς εντολές και για τον 2ο user 🡪 Geo**

****

**E3:**

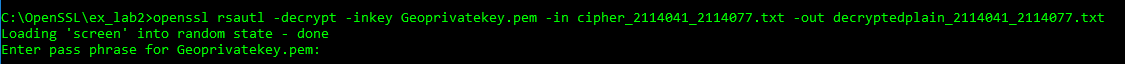
**Κρυπτογράφηση Viglas\_Papadopoulos.txt με το public key του user Geo** **και δημιουργία κρυπτογραφημένου μηνύματος στο** **cipher\_2114041\_2114077.txt:**

«openssl rsautl –encrypt –pubin –inkey Geopublickey.pem –in Viglas\_Papadopoulos.txt –out cipher\_2114041\_2114077.txt »



**Αποκρυπτογράφηση του cipher\_2114041\_2114077.txt με το private key του user Geo και δημιουργία αποκρυπτογραφημένου μηνύματος στο decryptian\_2114041\_2114077.txt:**

«openssl rsautl –decrypt –inkey Geoprivatekey.pem –in cipher\_2114041\_2114077.txt –out decryptedplain\_2114041\_2114077.txt»

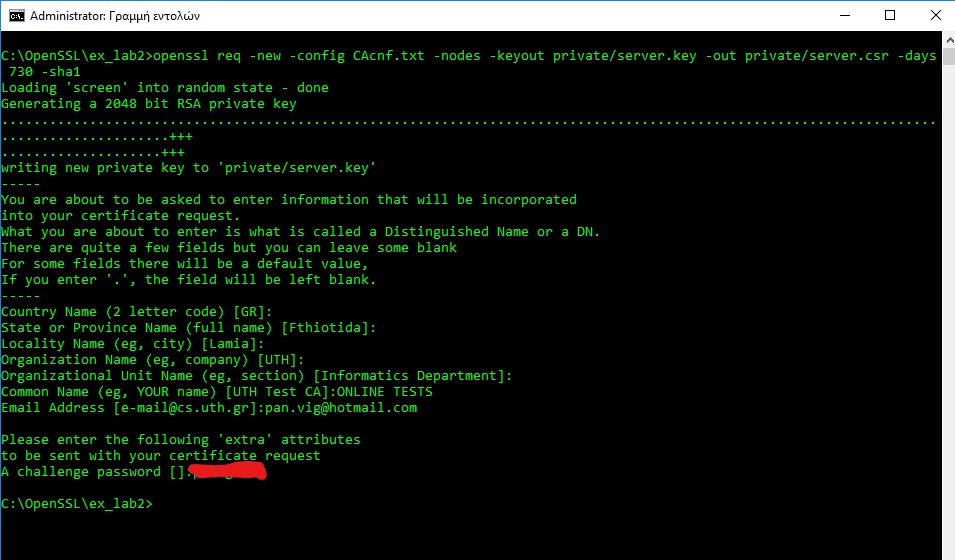


**E4:**

Δημιουργία αίτησης πιστοποίησης προς την Α.Π. για 730 μέρες με, sha1:

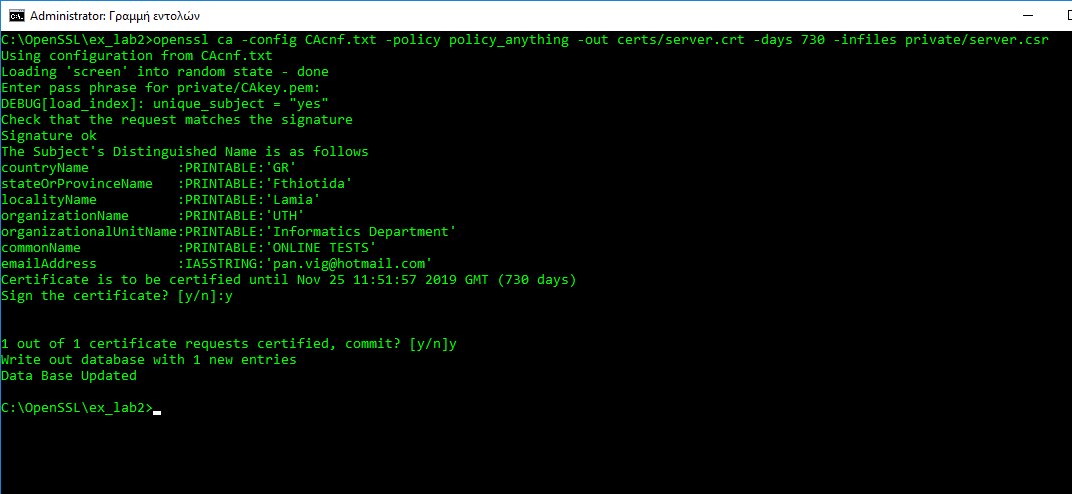
* Τα αρχεία server.key και server.csr δημιουργούνται κ αποθηκεύονται στον φάκελο private!
* Μπαίνει από default RSA, 2048bits, αφού παίρνει τις τιμές από το CAcnf.txt

« openssl req -new -config CAcnf.txt -nodes -keyout private/server.key -out private/server.csr -days 730 -sha1 »



Υπογραφή αίτησης από την Α.Π. για 730 μέρες:

« openssl ca -config CAcnf.txt -policy policy\_anything -out certs/server.crt -days 730 -infiles private/server.csr »



**E5:**

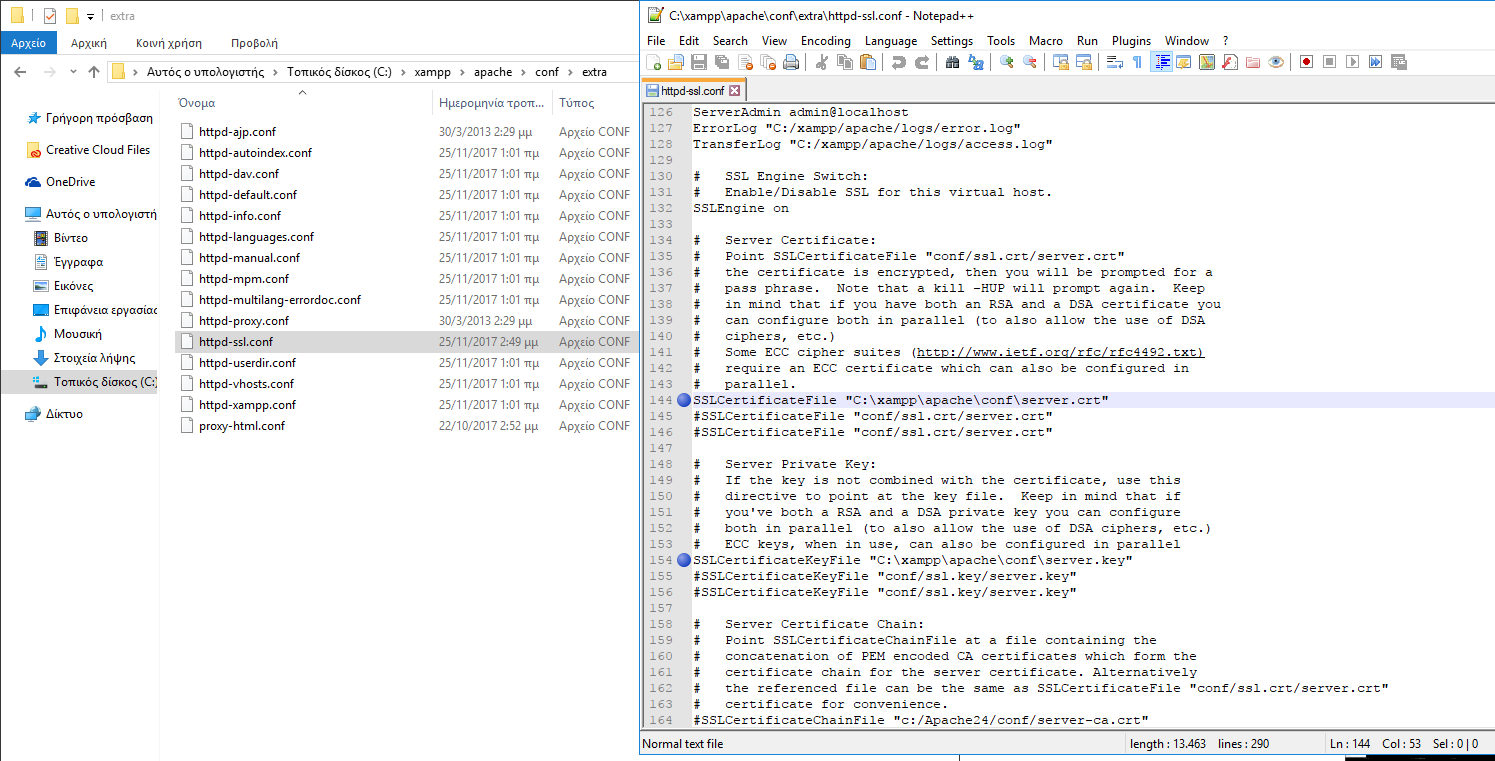
Πήραμε τα νέα (αυτά που κάναμε στο Ε4) “server.key” “server.crt”, τα βάλαμε στον φάκελο του apache 🡪C:\xampp\apache\conf

Και μετά επεξεργαστήκαμε το αρχείο «httpd-ssl.conf» του path “C:\xampp\apache\conf\extra” κ βάλαμε να «κοιτάει» στα path του νέου κλειδιού και πιστοποίητικού.

**httpd-ssl.conf πριν την αλλαγή:**

****

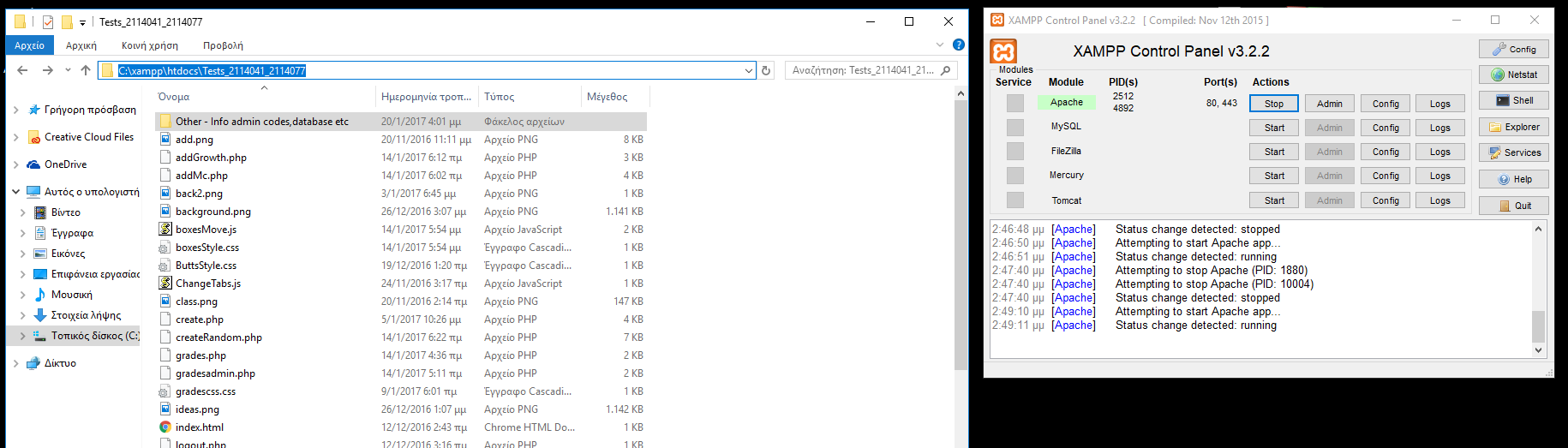
**httpd-ssl.conf μετά την αλλαγή:**

****

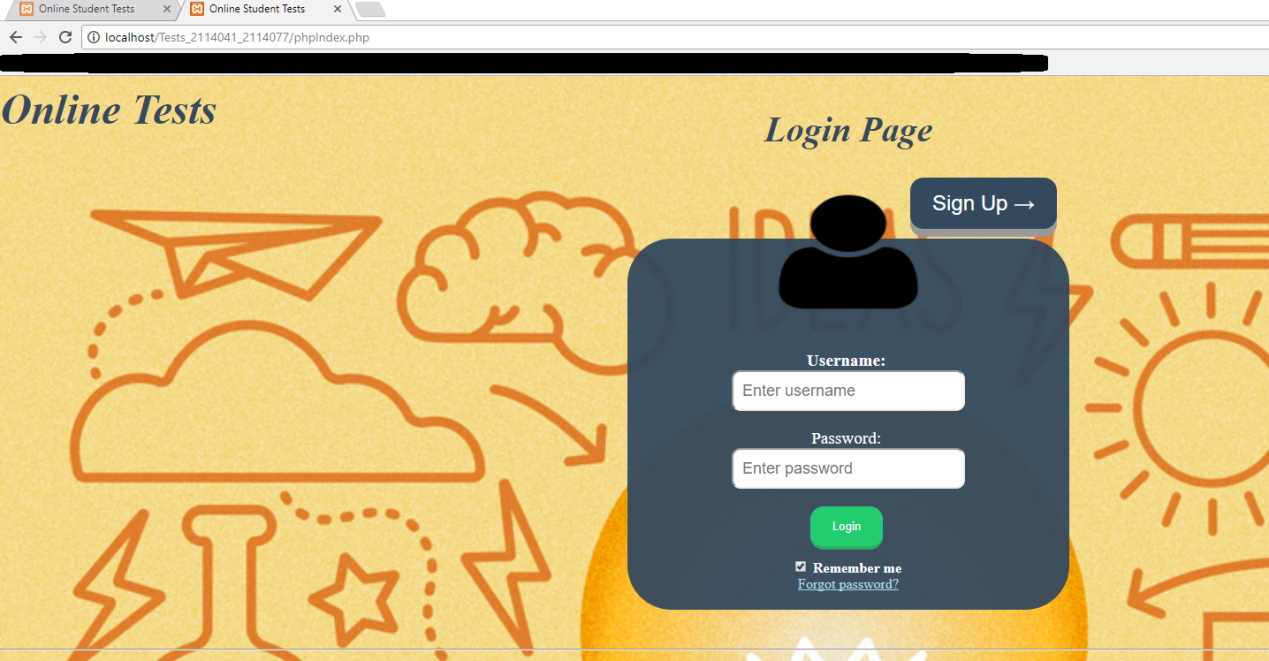
**New server key – crt:**

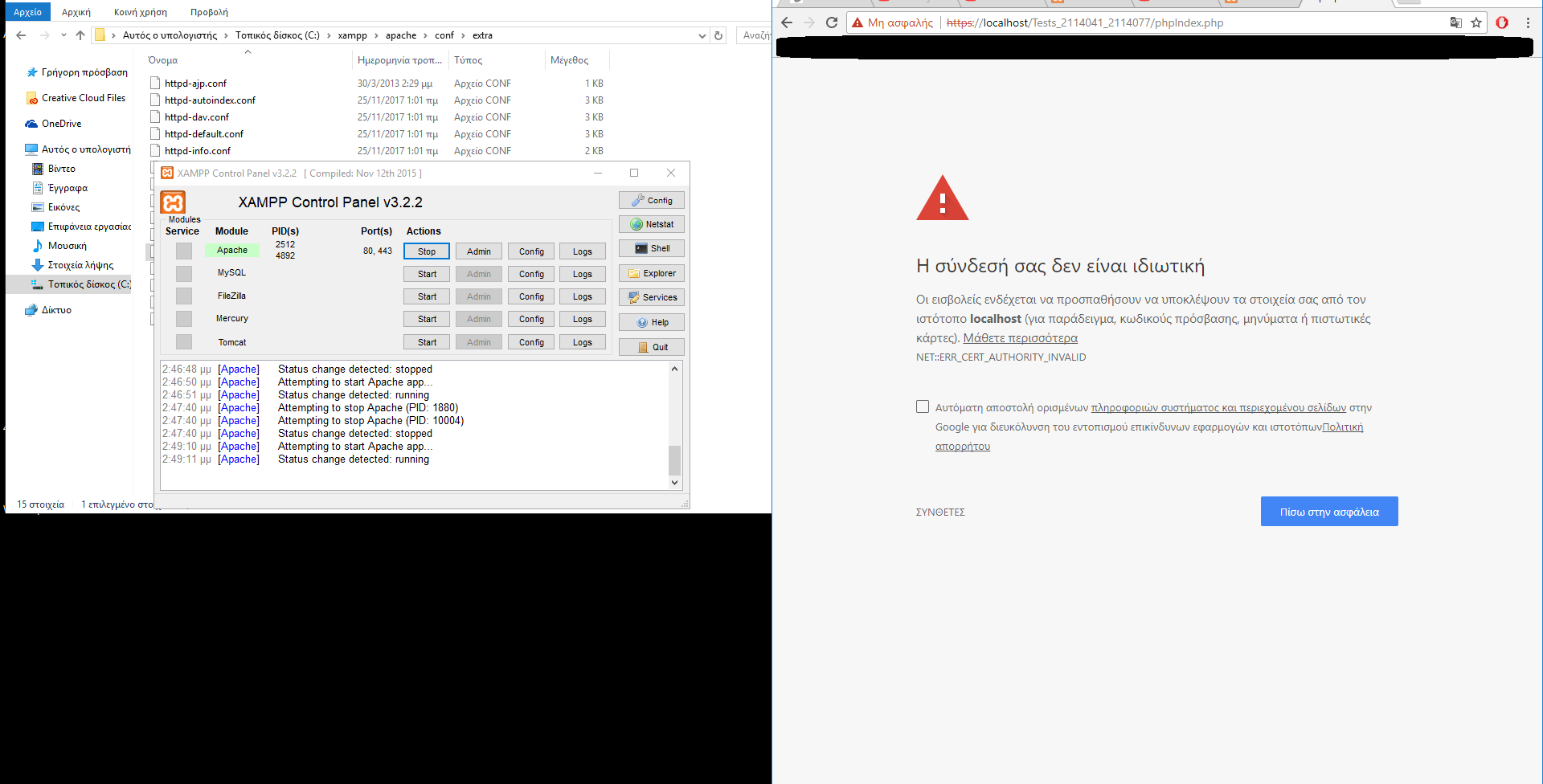
****

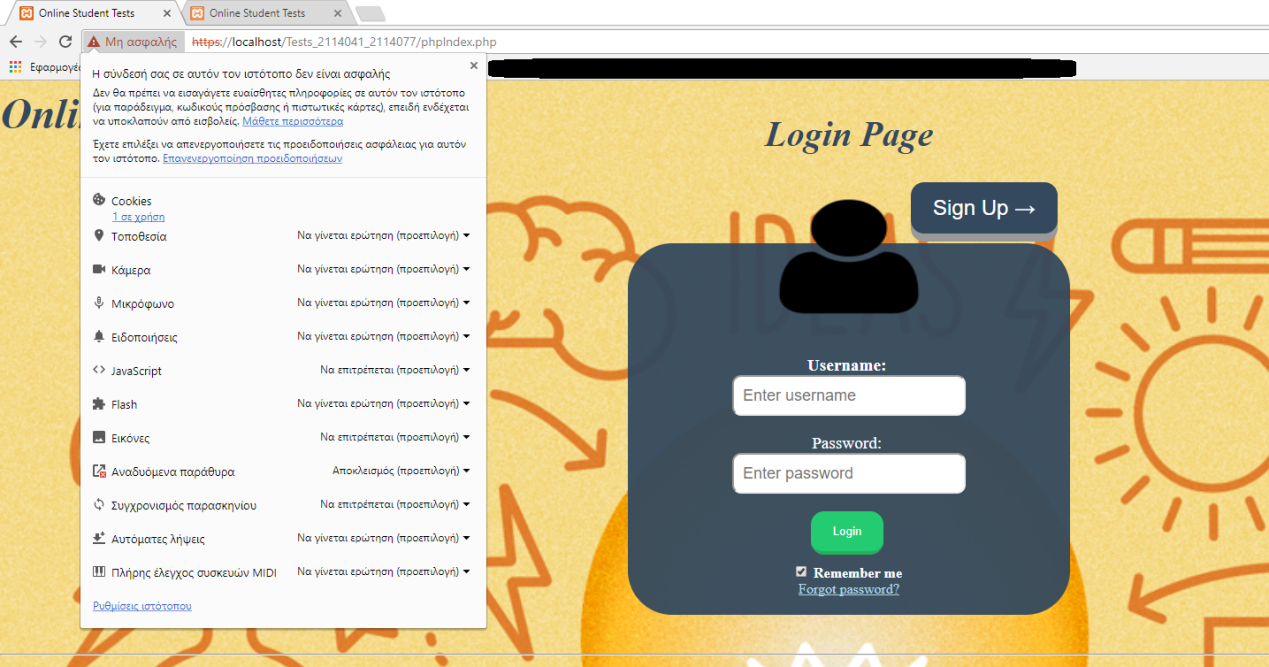
**Web files path:**

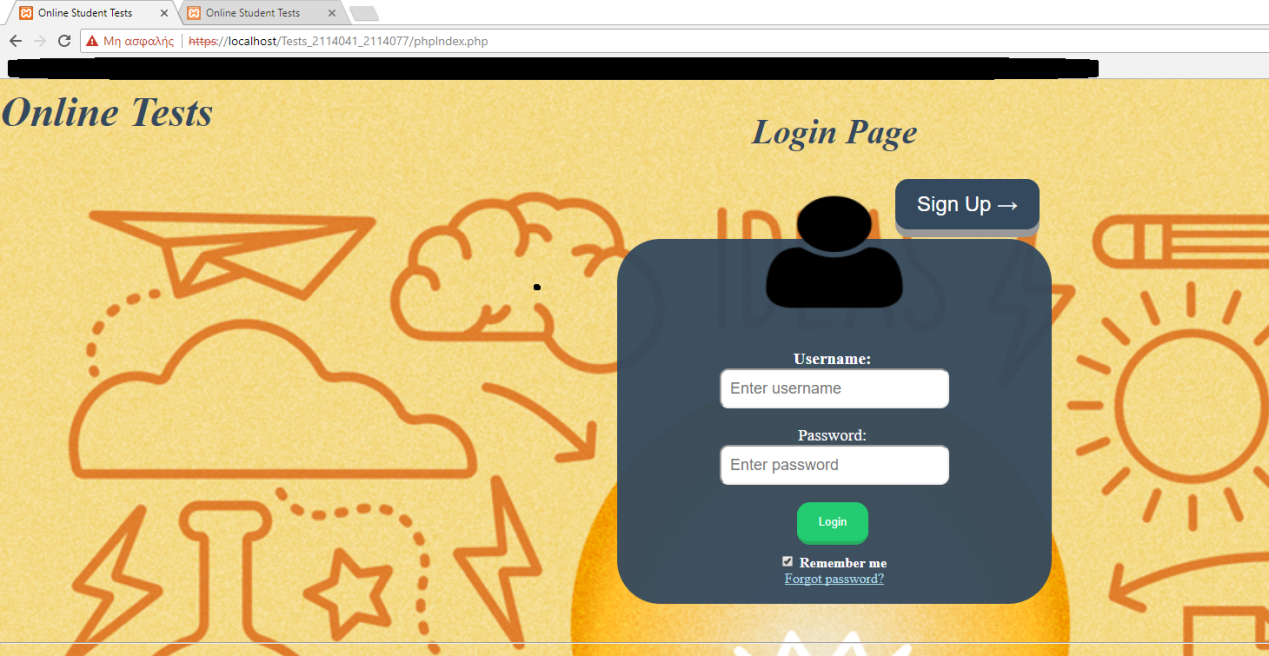
****

**Web Page http/https:**

****

****

****

****

**Σχόλιο: Συνδεθήκαμε στη σελίδα, χρησιμοποιώντας το δικό μας πιστοποιητικό. Αλλά το βγάζει κόκκινο, διότι δεν είναι αναγνωρισμένο.**