

**exercise 2**  
**openssl**

José A. Mañas < <http://www.dit.upm.es/~pepe/> >  
Dep. de Ingeniería de Sistemas Telemáticos  
E.T.S. Ingenieros de Telecomunicación  
Universidad Politécnica de Madrid

**18 September 2016**

- OpenSSL
  - already installed: linux, mac os x
  - site: <https://www.openssl.org/>
  - windows: <https://sourceforge.net/projects/openssl/>

1. prepare (or download) configuration file
  - <http://www.dit.upm.es/~pepe/doc/seg4/ca/openssl.cnf>
2. download CA certificates
  - <http://www.dit.upm.es/~pepe/doc/seg4/ca/ca.crt>
  - [http://www.dit.upm.es/~pepe/doc/seg4/ca/ca\\_cert.pem](http://www.dit.upm.es/~pepe/doc/seg4/ca/ca_cert.pem)
3. generate key pair (X = NameSurname)
  - `openssl req -config openssl.cnf  
-out X.csr -new -newkey rsa:2048 -nodes -keyout X_sec.pem`
4. send X.csr to jmanas@dit.upm.es

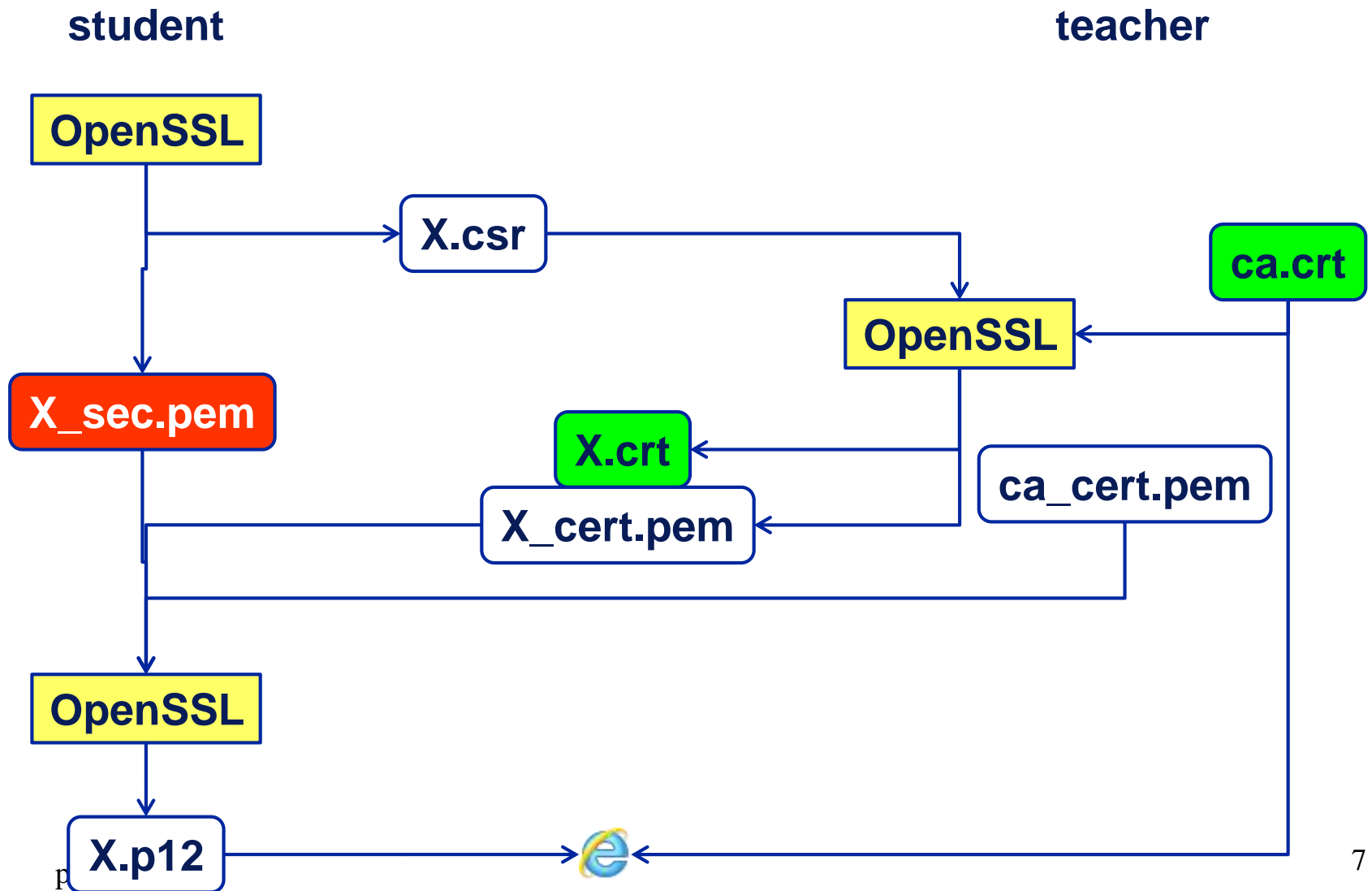
6. you will receive an email with the certificate in two formats
  - X\_cert.pem (PEM)
  - X.crt (DER)
7. merge with private key
  - `openssl pkcs12 -export -out X.p12 -inkey X_sec.pem -in X_cert.pem -certfile ca_cert.pem`
8. file X.p12 is a password-protected container
  - private key
  - public key
  - certificate

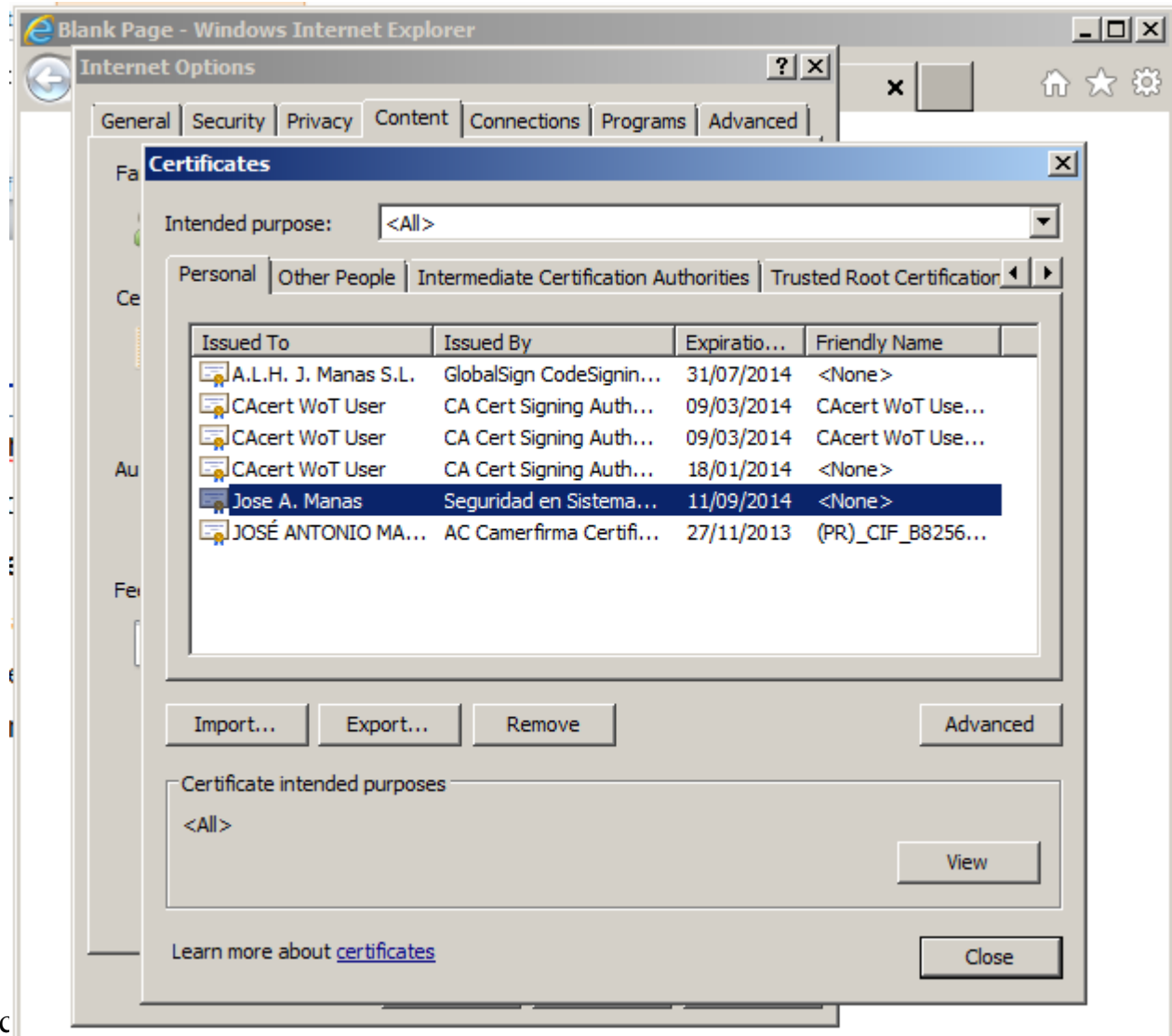
- view certificate

```
openssl x509 -in X_cert.pem -noout -text
```

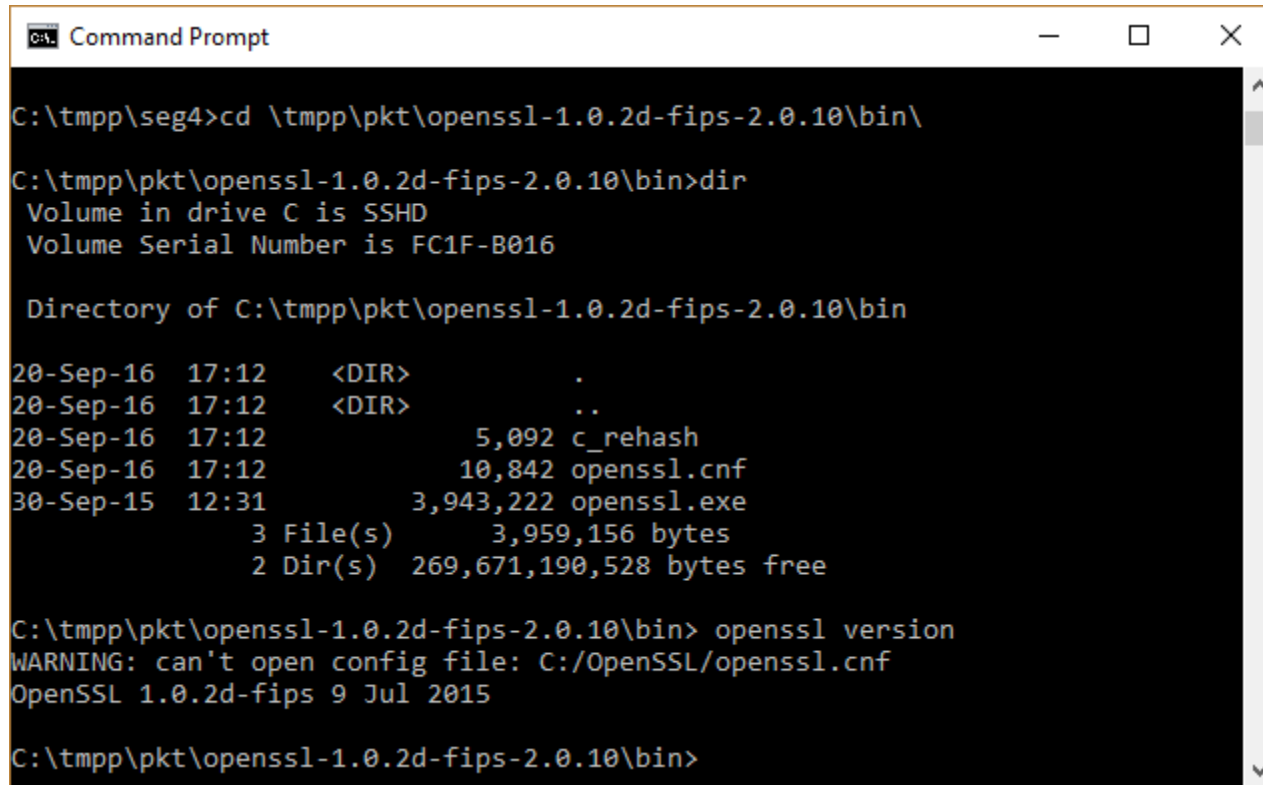
```
openssl x509 -inform der -in X.crt -noout -text
```

9. import .p12
  - en Windows, Internet Explorer,
  - mac, Keychain
    1. import CA certificate  
ca.crt
    2. import yours keys  
X.p12









```
Command Prompt

C:\tmpp\seg4>cd \tmpp\pkt\openssl-1.0.2d-fips-2.0.10\bin\

C:\tmpp\pkt\openssl-1.0.2d-fips-2.0.10\bin>dir
Volume in drive C is SSHD
Volume Serial Number is FC1F-B016

Directory of C:\tmpp\pkt\openssl-1.0.2d-fips-2.0.10\bin

20-Sep-16  17:12    <DIR>          .
20-Sep-16  17:12    <DIR>          ..
20-Sep-16  17:12                5,092 c_rehash
20-Sep-16  17:12               10,842 openssl.cnf
30-Sep-15  12:31           3,943,222 openssl.exe
               3 File(s)          3,959,156 bytes
               2 Dir(s)  269,671,190,528 bytes free

C:\tmpp\pkt\openssl-1.0.2d-fips-2.0.10\bin> openssl version
WARNING: can't open config file: C:/OpenSSL/openssl.cnf
OpenSSL 1.0.2d-fips 9 Jul 2015

C:\tmpp\pkt\openssl-1.0.2d-fips-2.0.10\bin>
```