dit-upm

criptografía

práctica 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 de septiembre de 2016

software

- OpenSSL
  - preinstalado: linux, mac os x
  - oficial: https://www.openssl.org/
  - windows: https://sourceforge.net/projects/openssl/

generación de claves y solicitud CSR

1. preparar el fichero de configuración (o descargarlo)
   - http://www.dit.upm.es/~pepe/doc/seg4/ca/openssl.cnf
2. descargar los certificados de la CA
   - http://www.dit.upm.es/~pepe/doc/seg4/ca/ca.crt
   - http://www.dit.upm.es/~pepe/doc/seg4/ca/ca_cert.pem
3. generar el par de claves (X = NombreApellidos)
   - openssl req -config openssl.cnf
     -out X.csr -new -newkey rsa:2048 -nodes -keyout X_sec.pem
4. enviar X.csr a jmanas@dit.upm.es

recepción del certificado

6. recibirá un email con el certificado
   - X_cert.pem (formato PEM)
   - X.crt (formato DER)
7. se combina con la clave privada
   - openssl pkcs12 -export
     -out X.p12 -inkey X_sec.pem -in X_cert.pem -certfile ca_cert.pem
8. El paquete X.p12 es un contenedor protegido por contraseña
   - clave privada
   - clave pública
   - certificado

otras funciones

- para ver el certificado

  openssl x509 -in X_cert.pem -noout –text

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

uso del certificado

9. cargamos el fichero .p12

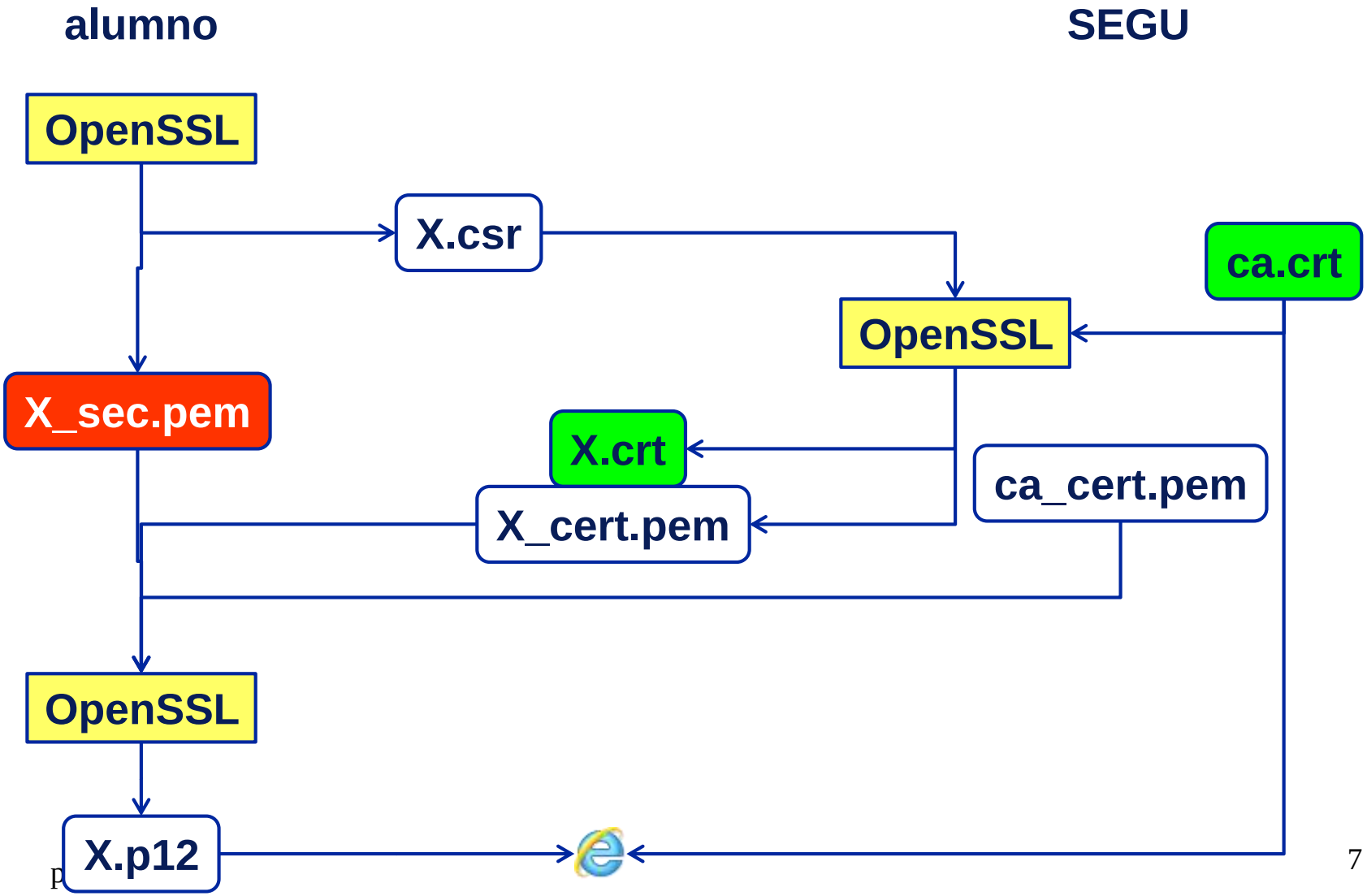
- en Windows, Internet Explorer,
- en mac, Keychain

  1. importe el certificado de la autoridad

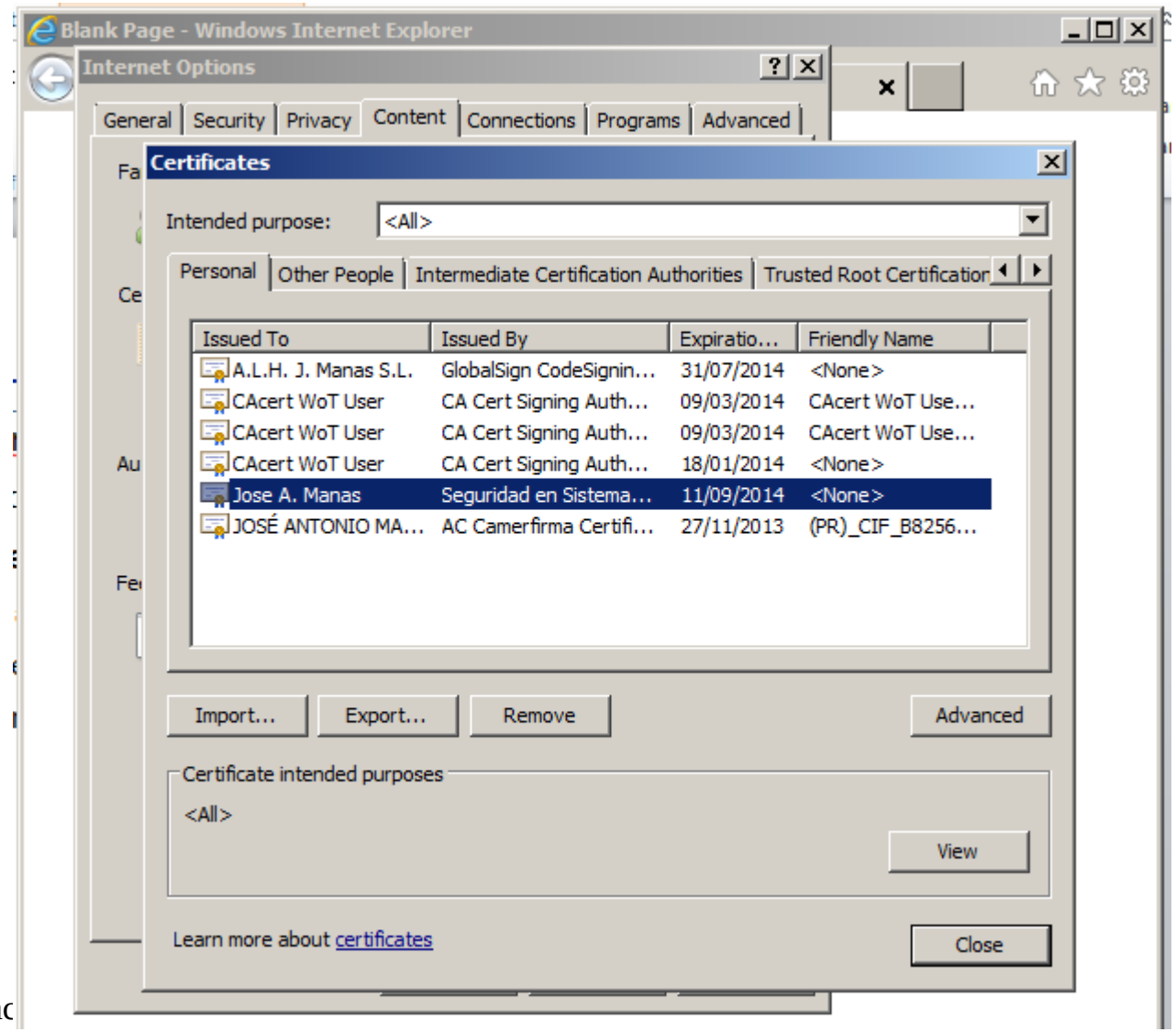
     ca.crt

  2. importe sus claves
     X.p12

pasos y ficheros



certificado en windows



openssl en windows

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>
```