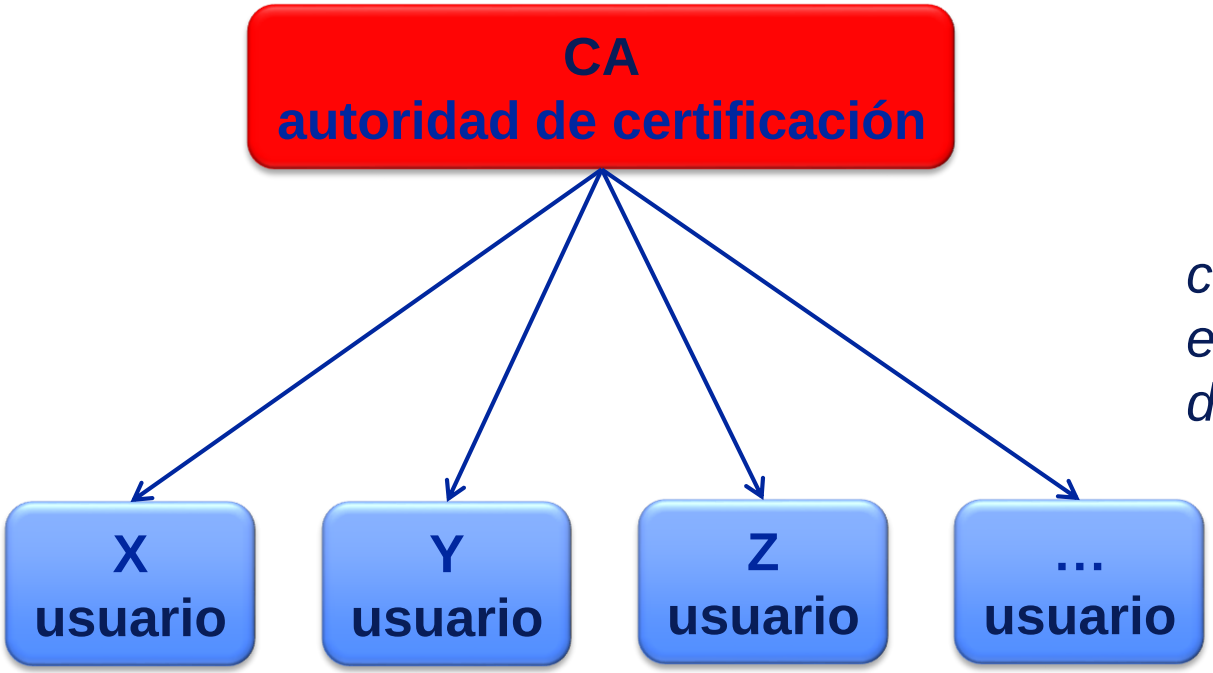
Autoridad de Certificación usando xca

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

15 de octubre de 2016

arquitectura



cada cajita es un ordenador diferente

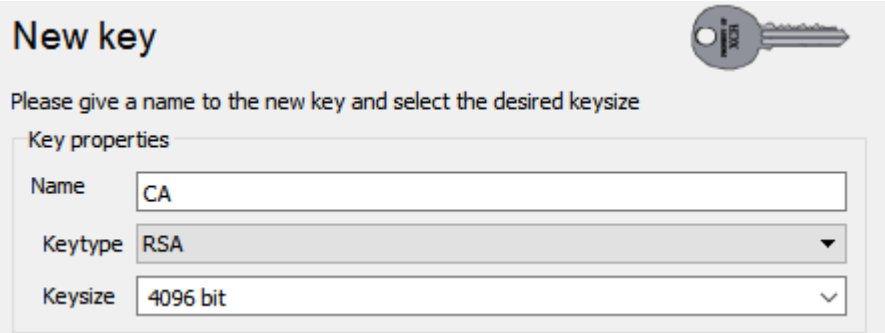
- perfil RFC 5280 (bastante habitual)

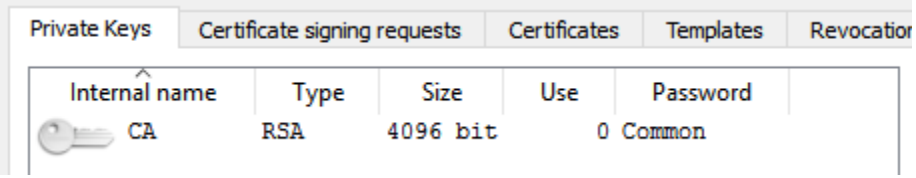
xca (OpenSSL)

1. descargar e instalar xcs (interfaz sobre openssl)
   - http://sourceforge.net/projects/xca/
   - http://xca.sourceforge.net/xca-14.html
2. prepare un directorio de trabajo
   - debe estar en las carpetas del alumno, con todos los derechos de lectura y escritura
3. Cree una nueva base de datos en ese directorio
   - File > New database

claves de la CA

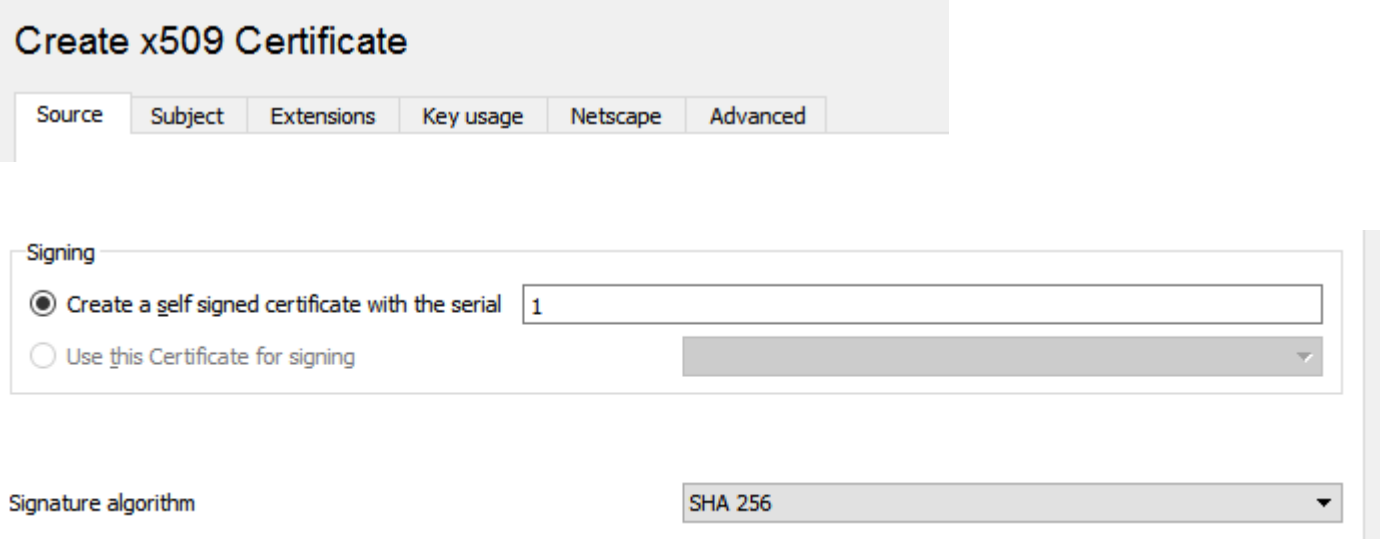
- creamos una clave RSA de 4096 bits





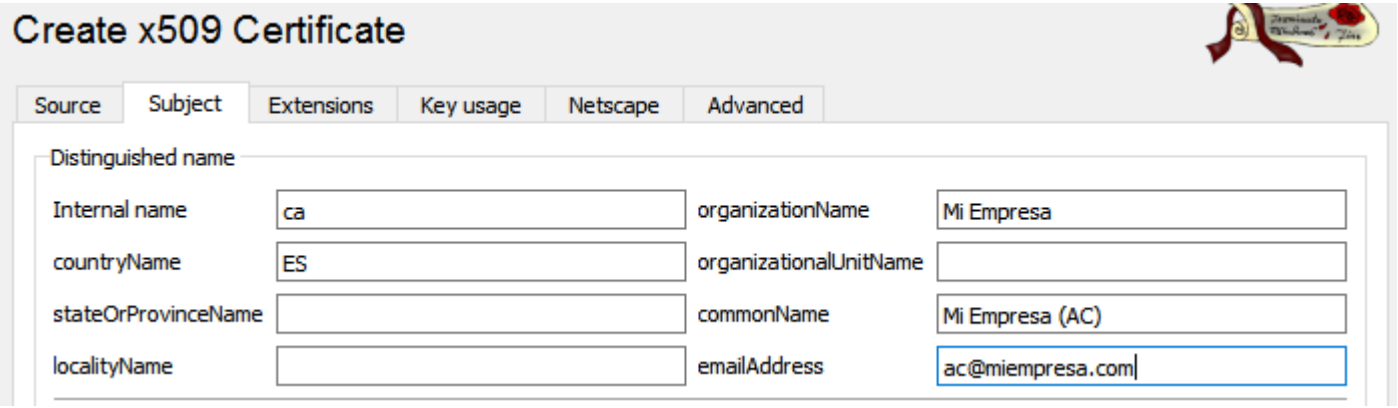
certificado de la CA

- genera un [auto] certificado



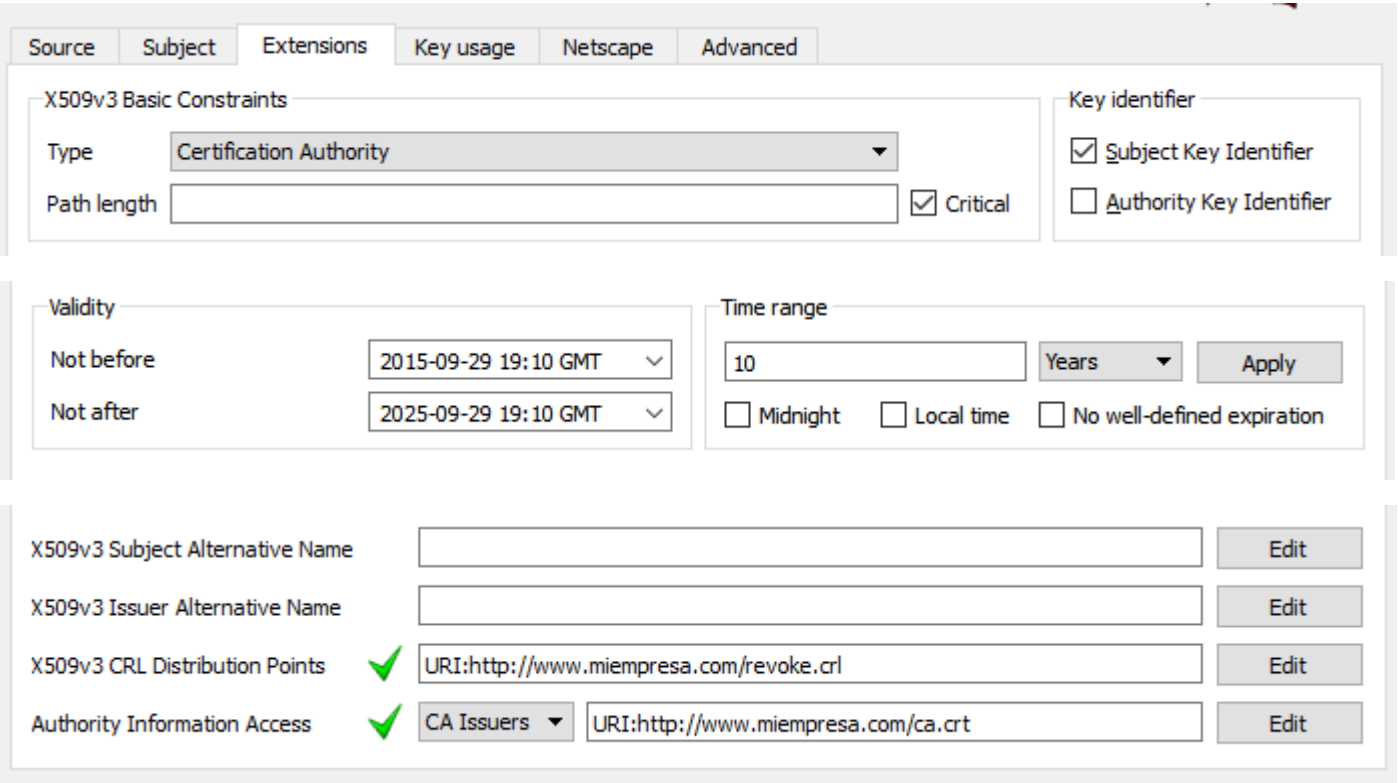
certificado de la CA

- genera un [auto] certificado



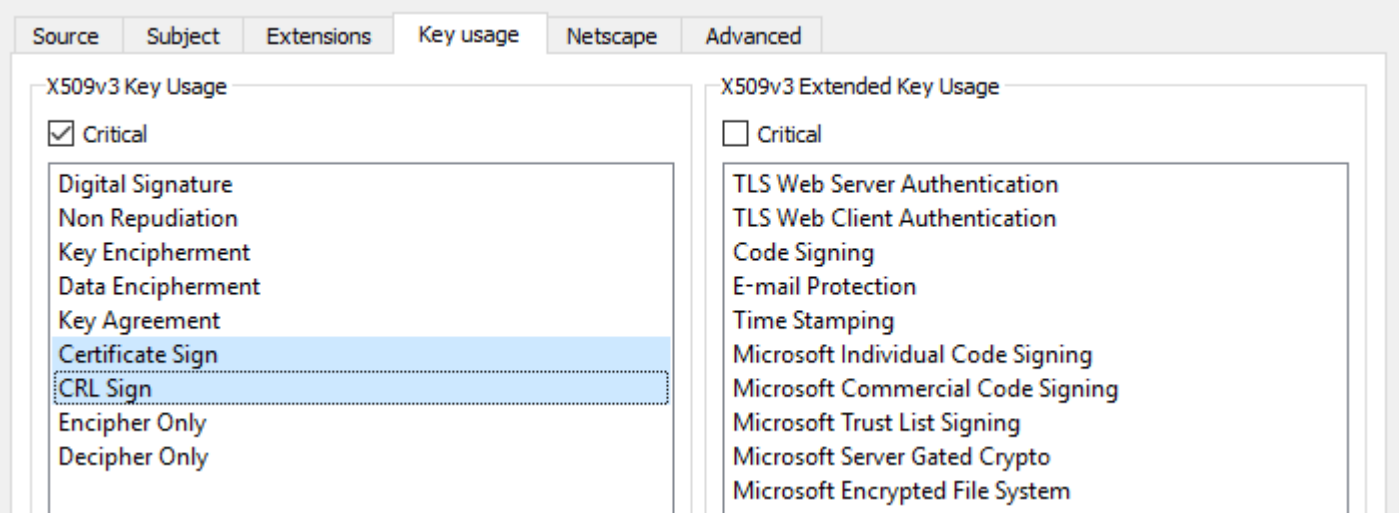
certificado de la CA

- genera un [auto] certificado
- se recurre a un perfil típico (RFC 5280)



certificado de la CA

- genera un [auto] certificado
- se recurre a un perfil típico (RFC 5280)

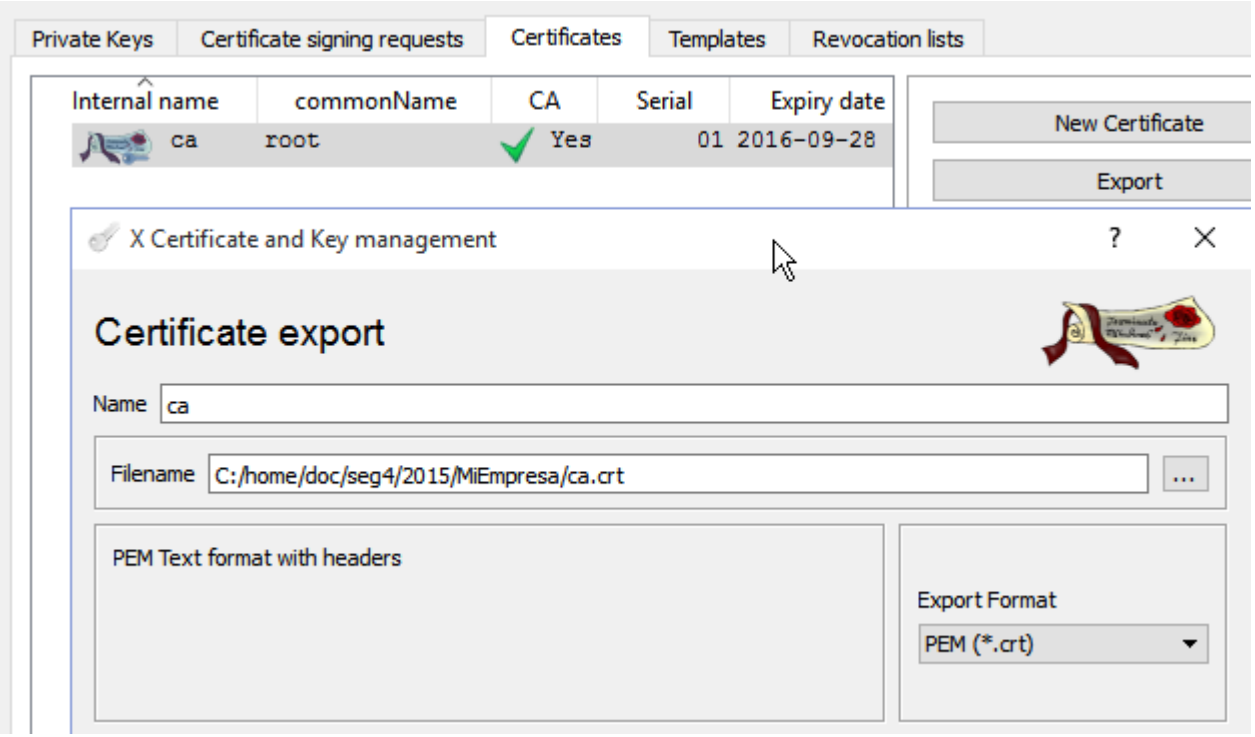


certificado de la CA

- genera un [auto] certificado

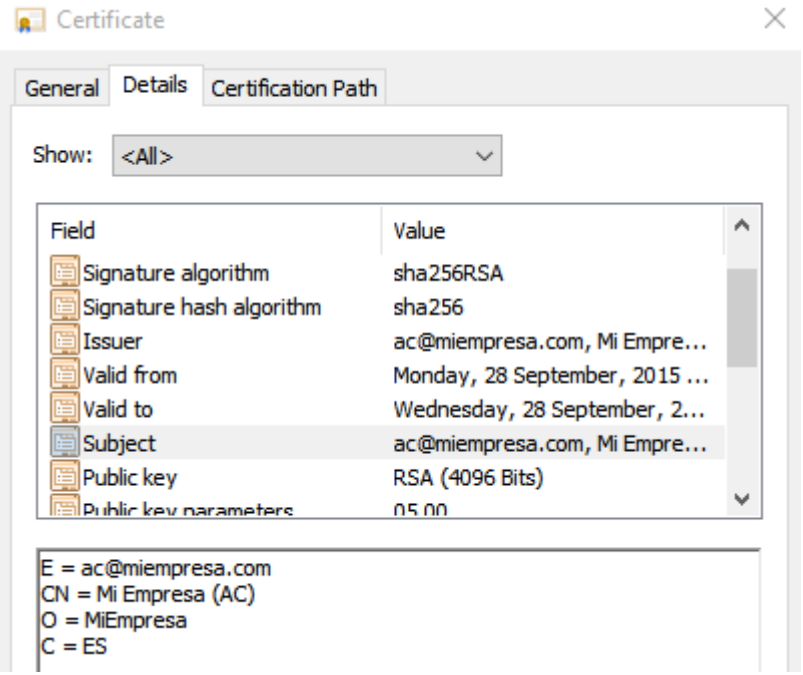
certificado de la CA

- genera un [auto] certificado



certificado de la CA

- genera un [auto] certificado

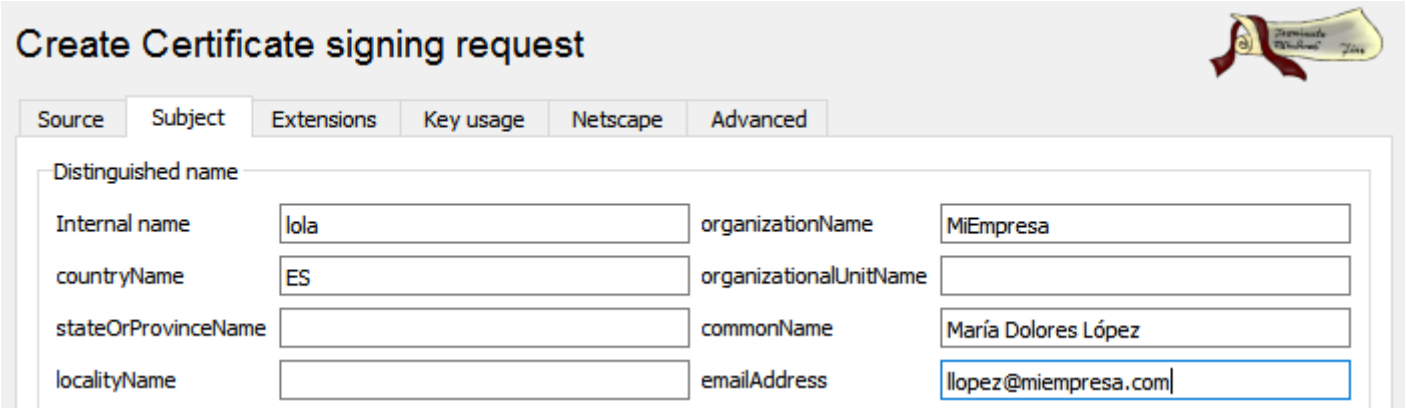


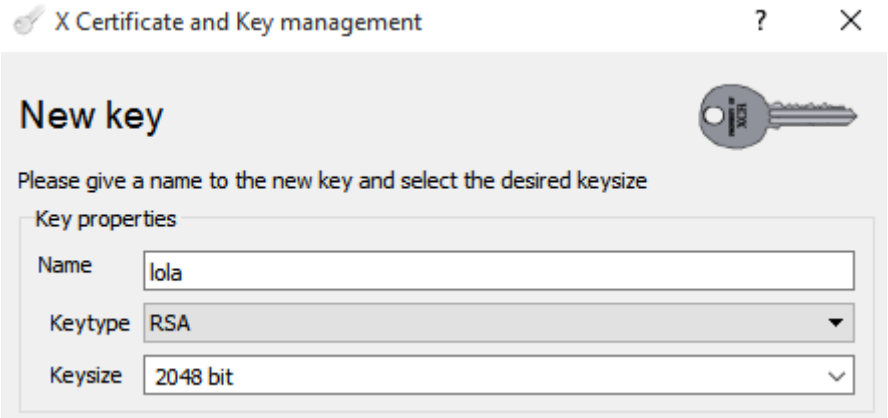
usuario X

- generación de claves y solicitud de certificado (csr)

usuario X

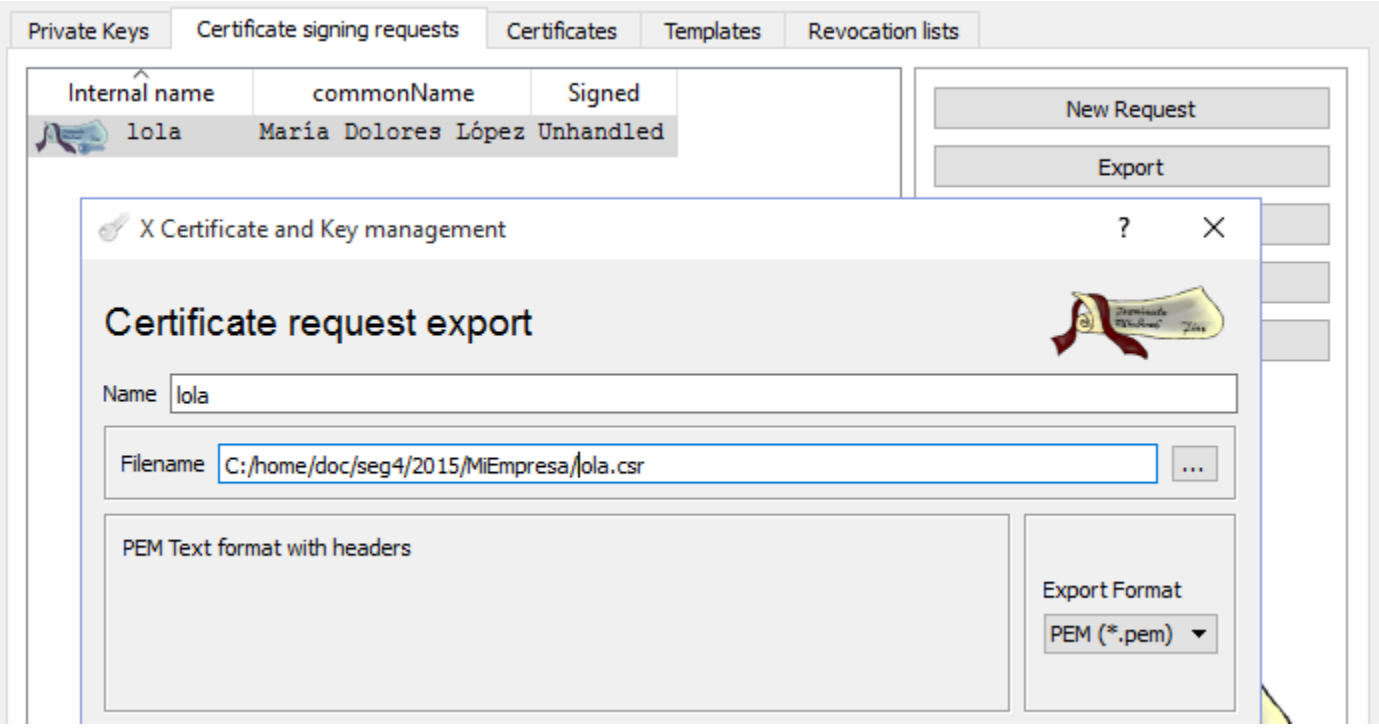
- generación de claves y solicitud de certificado (csr)





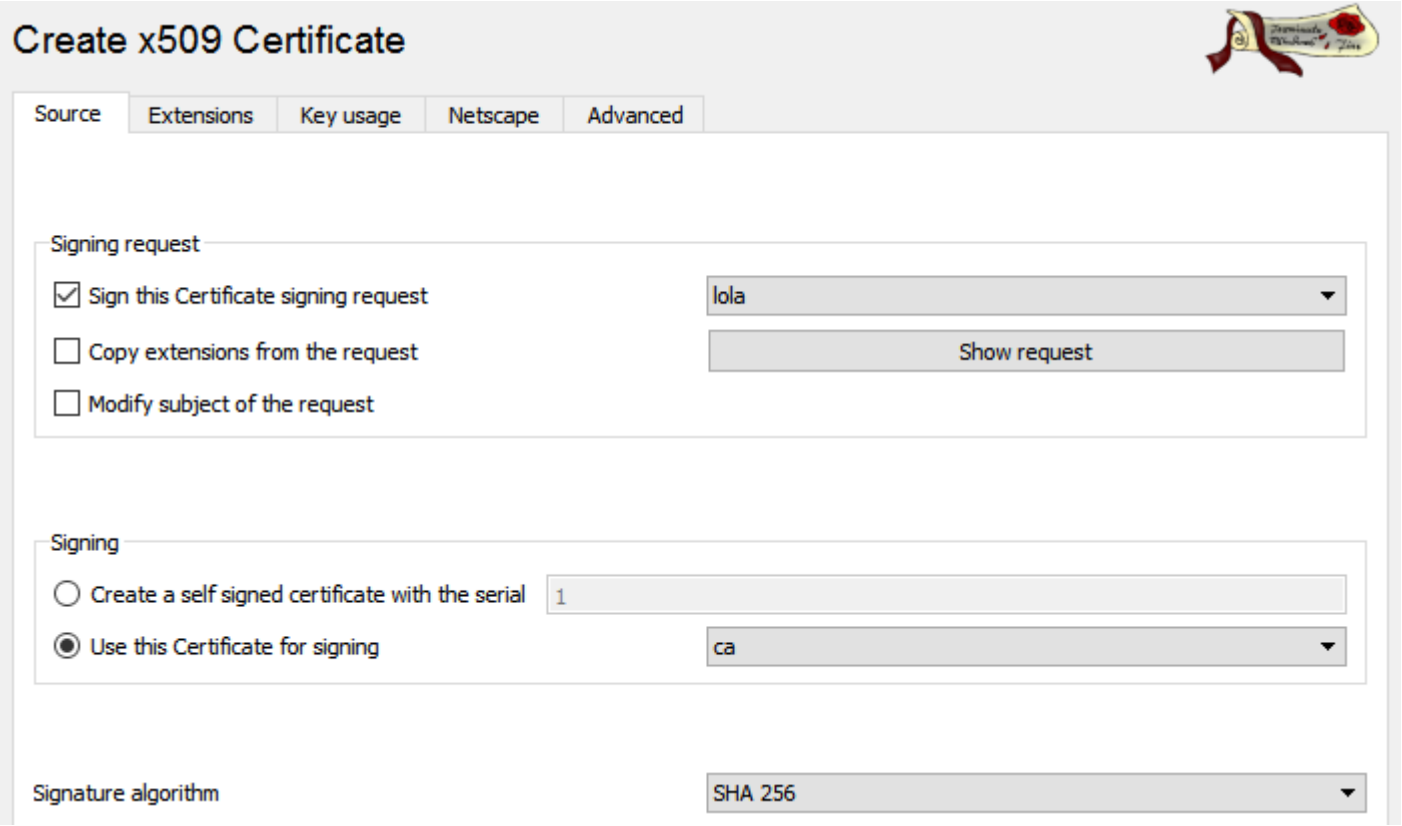
usuario X

- generación de claves y solicitud de certificado (csr)



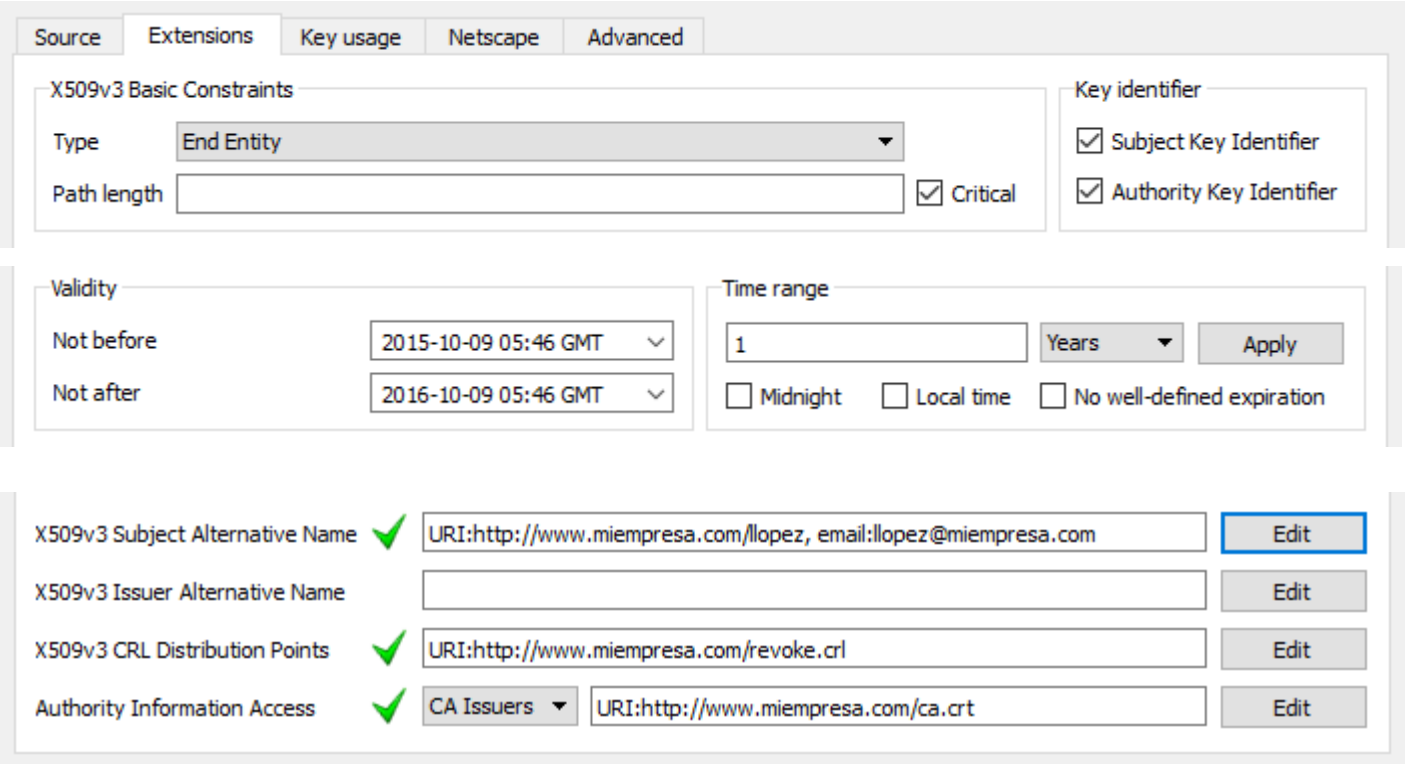
la CA certifica

- CA: genera el certificado (csr → cert)



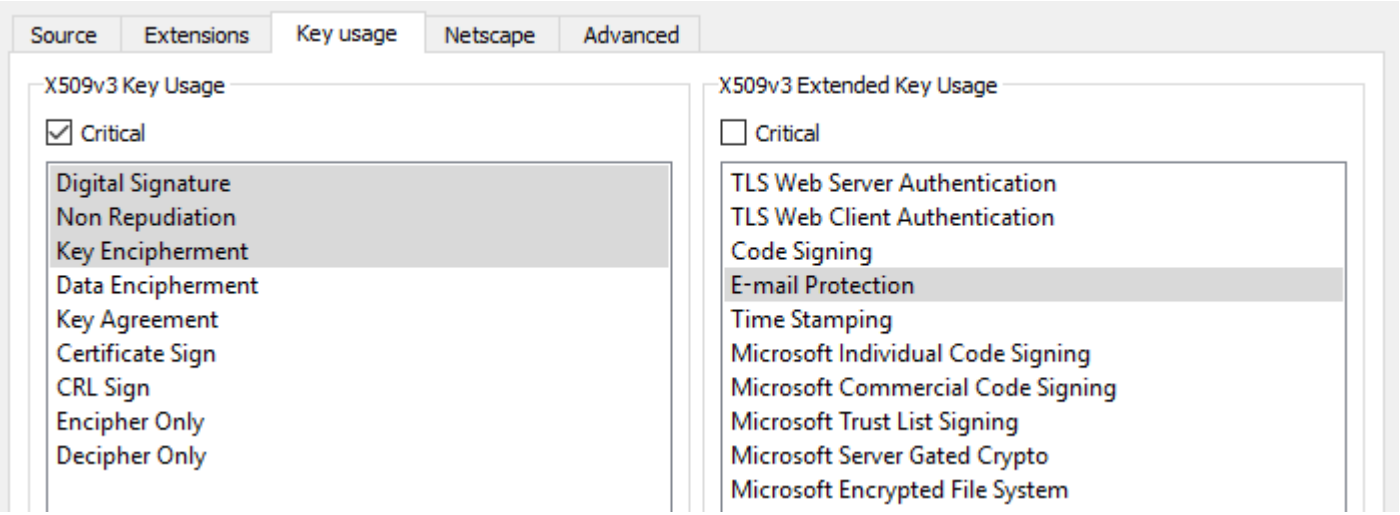
la CA certifica

- CA: genera el certificado (csr → cert)
- se recurre a un perfil típico (RFC 5280)



la CA certifica

- CA: genera el certificado (csr → cert)
- se recurre a un perfil típico (RFC 5280)



la CA certifica

- CA: genera el certificado (csr → cert)

Create x509 Certificate

Source | Extensions | Key usage | Netscape | Advanced

Other Tabs

X509v3 Basic Constraints critical:
CA:FALSE
X509v3 Subject Key Identifier:
C8:5A:A1:EC:2E:9A:D8:2F:5B:2C:D9:18:A3:45:86:DA:80:A7:93:68
X509v3 Authority Key Identifier:
keyid:01:0F:F9:57:00:46:CB:27:02:7B:51:68:F8:3D:9C:45:F6:84:43:12
DirName:/C=ES/O=Mi Empresa/CN=Mi Empresa (AC)/emailAddress=ac@miempresa.com
serial:01

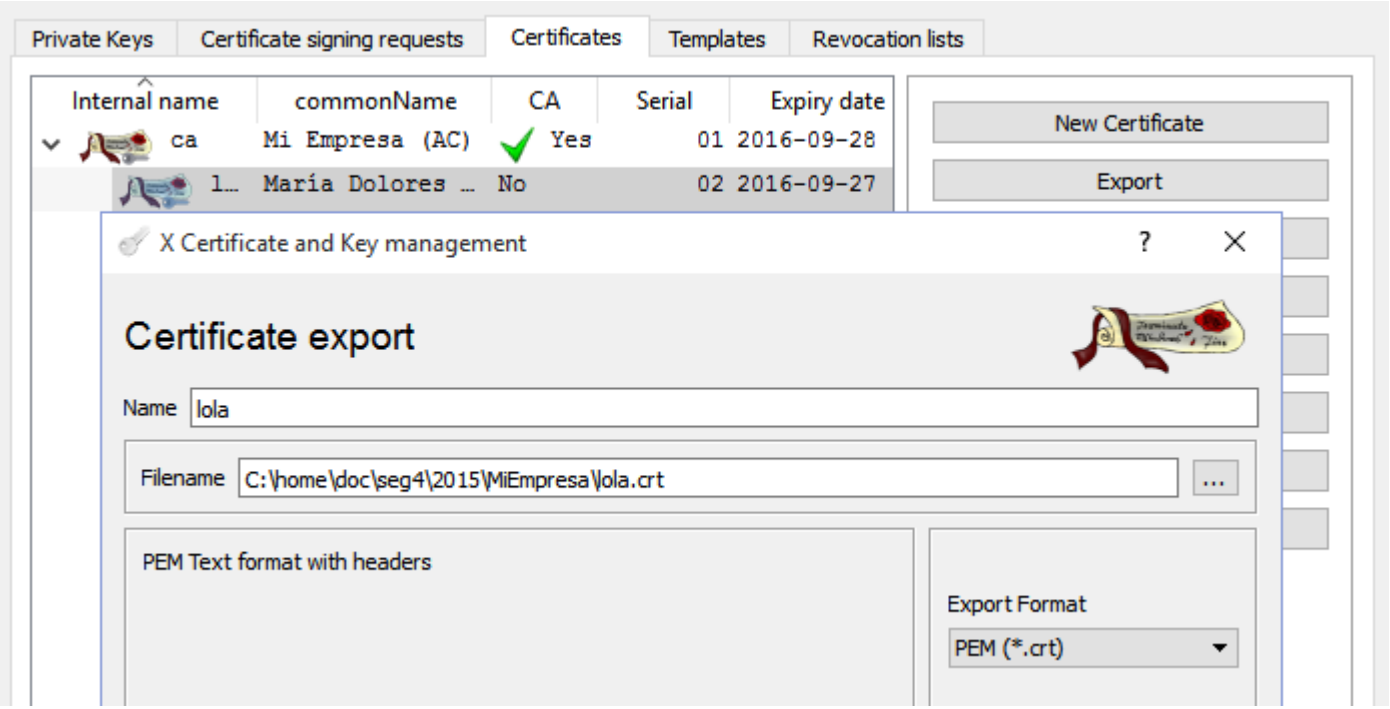
X509v3 Key Usage critical:
Digital Signature, Non Repudiation, Key Encipherment
X509v3 Extended Key Usage:
E-mail Protection
X509v3 Subject Alternative Name:
URI:http://www.miempresa.com/llopez, email:llopez@miempresa.com
X509v3 CRL Distribution Points:

Full Name:
URI:http://www.miempresa.com/revoke.crl

Authority Information Access:
CA Issuers - URI:http://www.miempresa.com/ca.crt

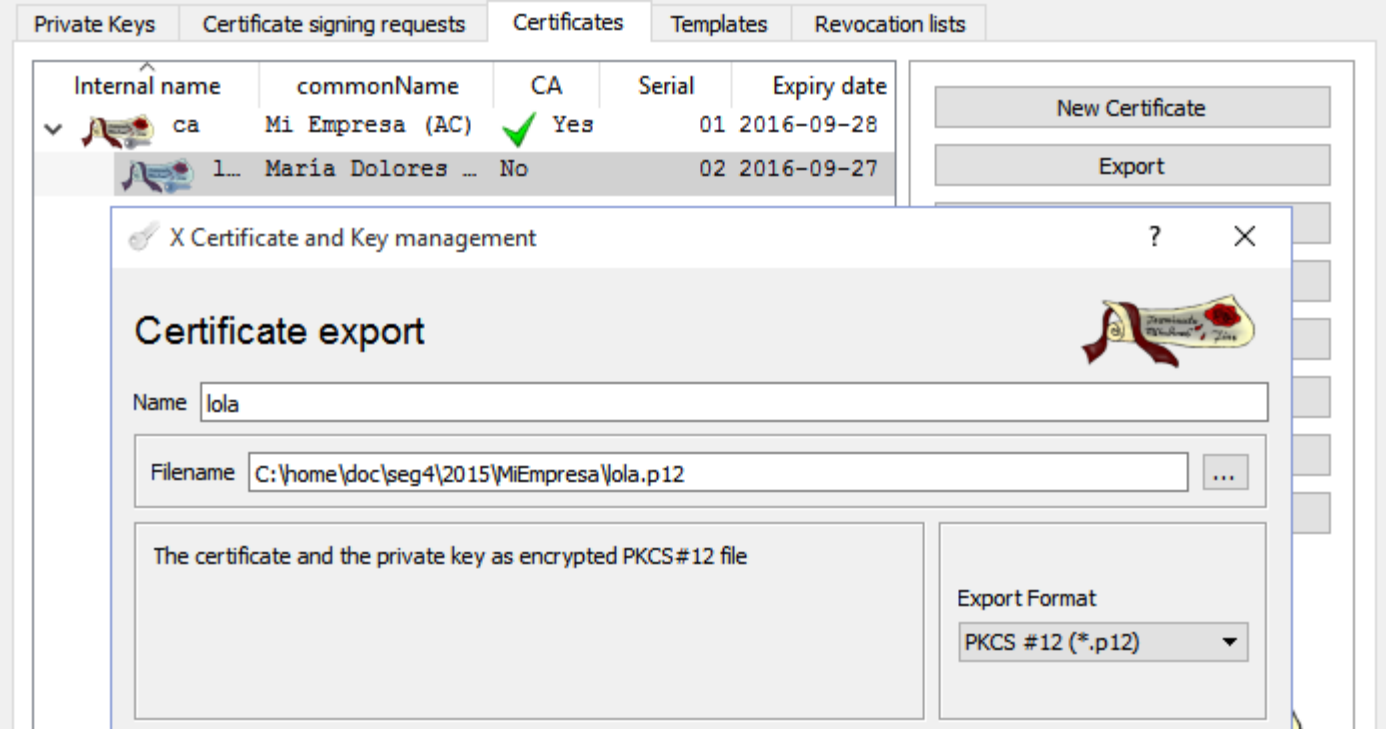
la CA certifica

- CA: genera el certificado (csr → cert)

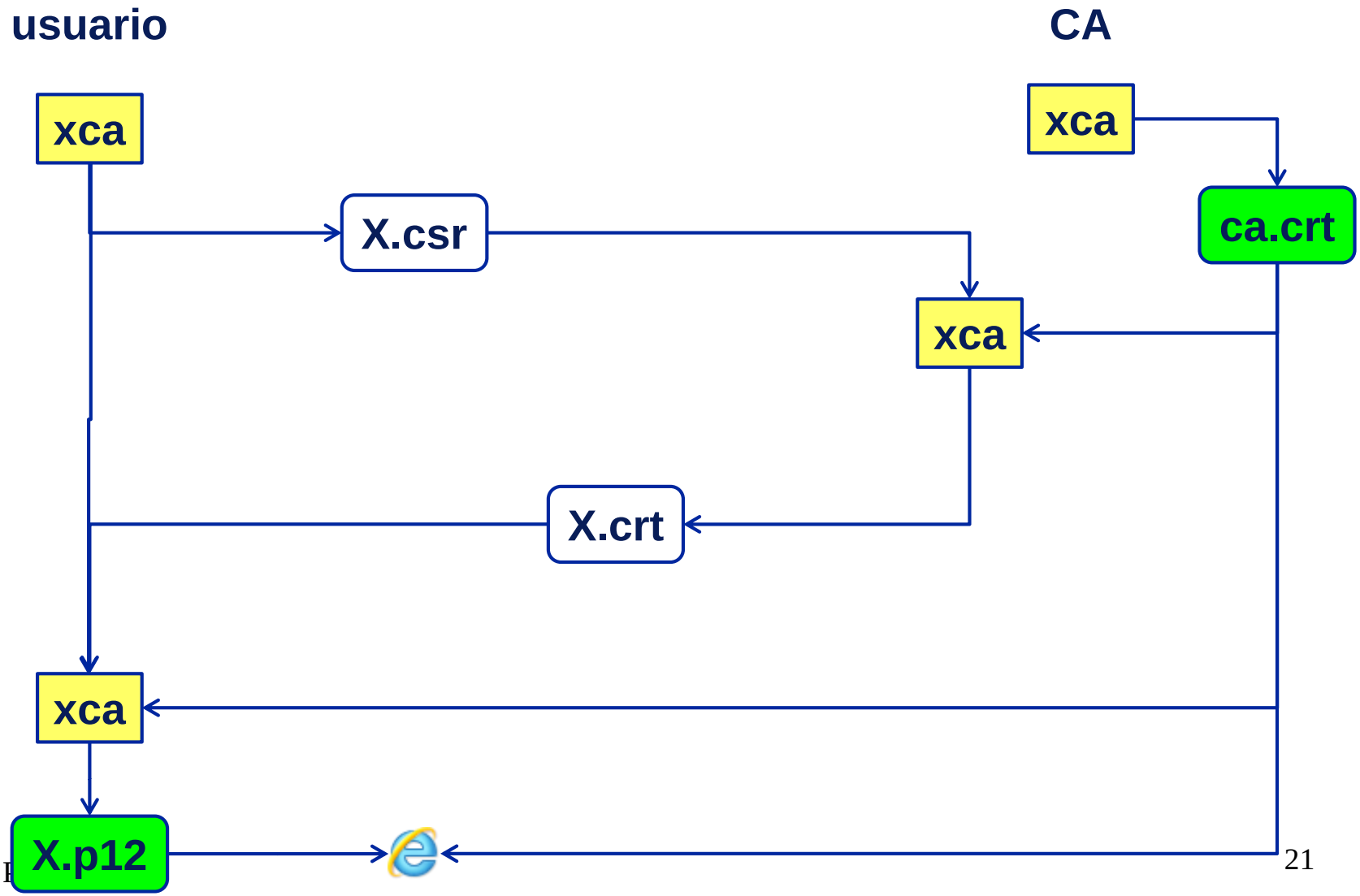


p12

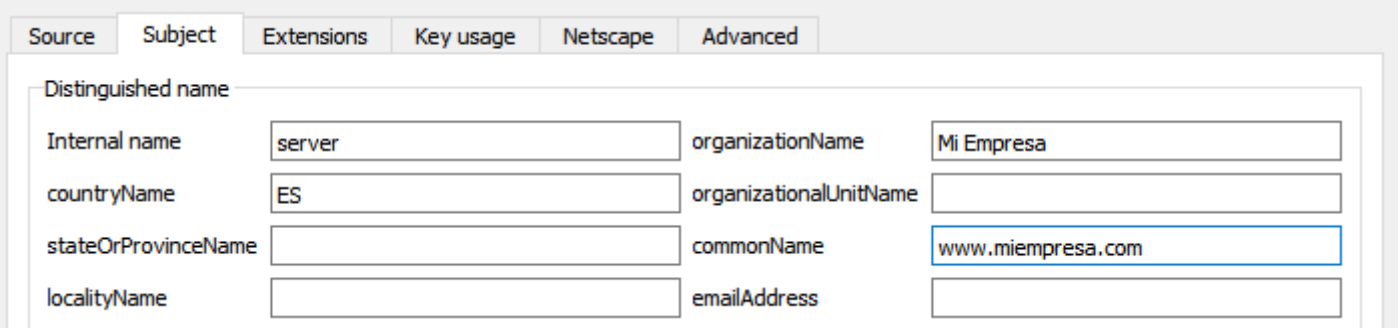
- exportar
  - exportar a p12 significa crear un paquete que agrupa la clave privada y los certificados del usuario (el propio y los que le avalan)
  - por contener una clave privada, se protege con una ontraseña que se pedirá cada vez que se quiera usar el p12
    (por ejemplo para cargarlo en el registro de certificados)



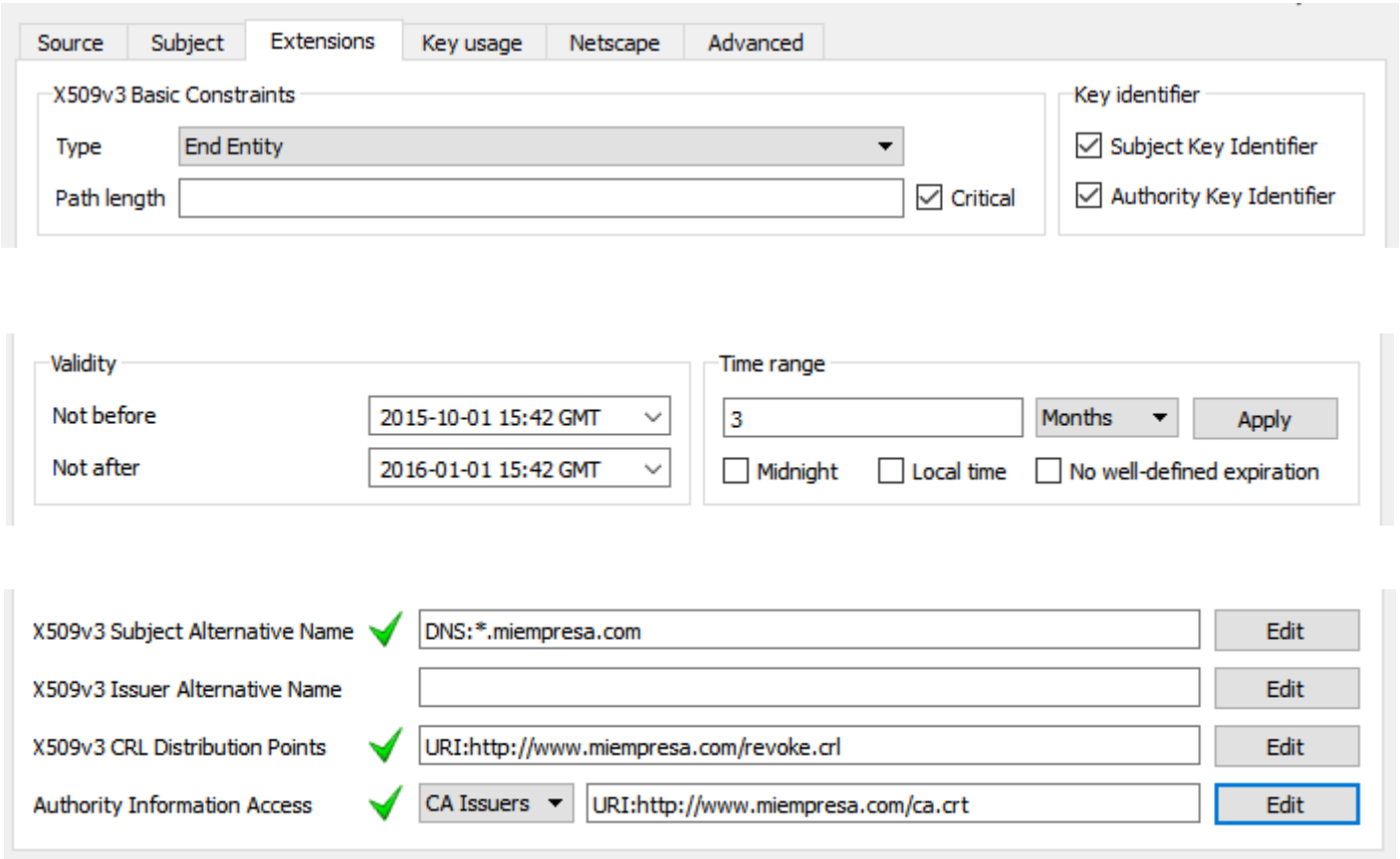
pasos y ficheros



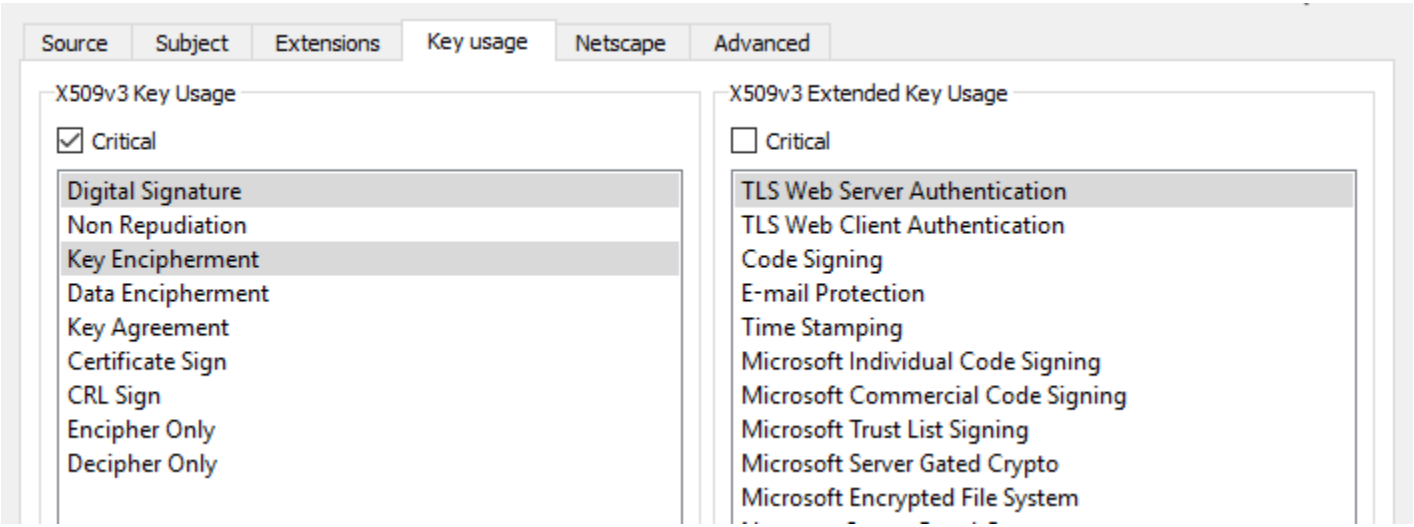
servidor https



servidor https



servidor https



servidor https

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Other Tabs

X509v3 Basic Constraints critical:
CA:FALSE
X509v3 Subject Key Identifier:
9D:AC:30:51:44:ED:80:7A:DA:C2:37:C6:C6:DB:02:DD:6F:84:8A:E1
X509v3 Authority Key Identifier:
keyid:01:0F:F9:57:00:46:CB:27:02:7B:51:68:F8:3D:9C:45:F6:84:43:12
DirName:/C=ES/O=Mi Empresa/CN=Mi Empresa (AC)/emailAddress=ac@miempresa.com
serial:01

X509v3 Key Usage critical:
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:*.miempresa.com
X509v3 CRL Distribution Points:

Full Name:
URI:http://www.miempresa.com/revoke.crl

Authority Information Access:
CA Issuers - URI:http://www.miempresa.com/ca.crt