dit-upm

criptografía

práctica 2

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

ejercicios

1. Firma de PDF con uno de …
   a) DNI electrónico
   b) certificado digital gratuito (CAcert)
   c) autoridad de certificación (CA) de la asignatura

Firma de PDF

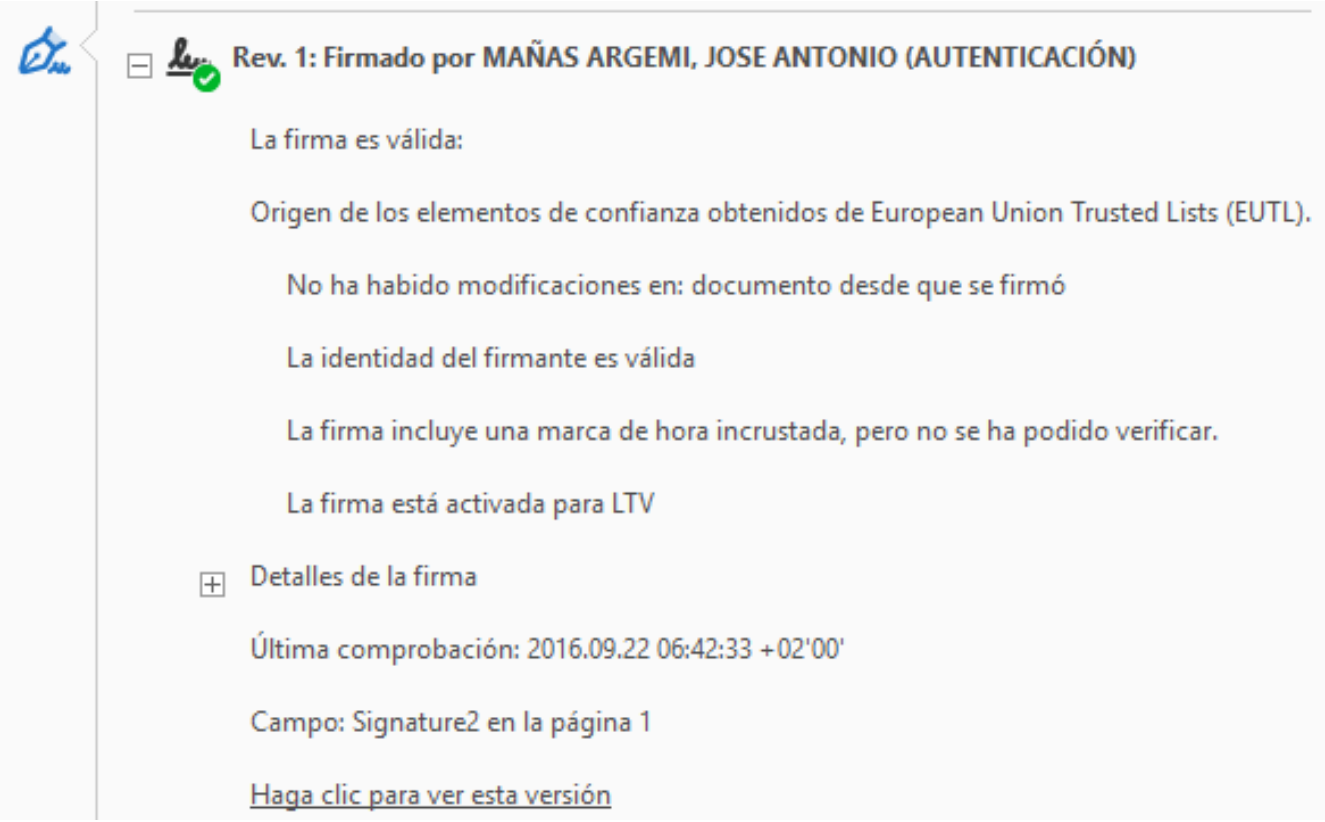
- Objetivo
  - aplicación de firma digital para autenticar documentos PDF
- Opciones: elegir una (o más) de …
  a) DNIe – para los que tienen DNIe y lector
  b) CAcert
  c) OpenSSL

firma de PDF

- Software (opciones)
  - Adobe Acrobat Reader
  - Xolido -- http://www.xolido.com/lang/
    - Xolido Sign Escritorio (gratuito)
  - JSignPdf -- http://jsignpdf.sourceforge.net/
- Tarea
  1. Se toma un fichero cualquiera en PDF
  2. Se firma incluyendo sello de tiempo
  3. Se envía al profesor jmanas@dit.upm.es

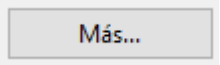
características de la firma

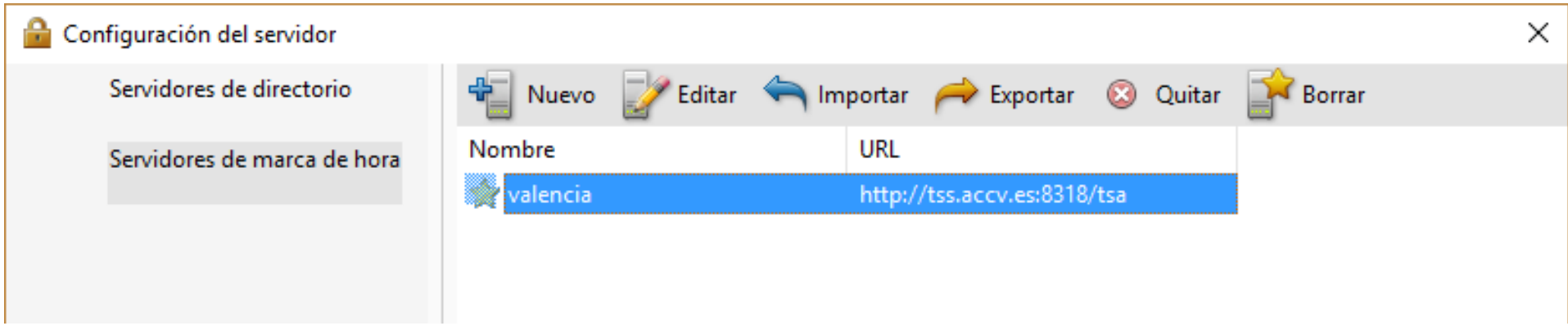
- No se exige, pero se recomienda que sea LTV
- Se exige sello de tiempo (timestamp)



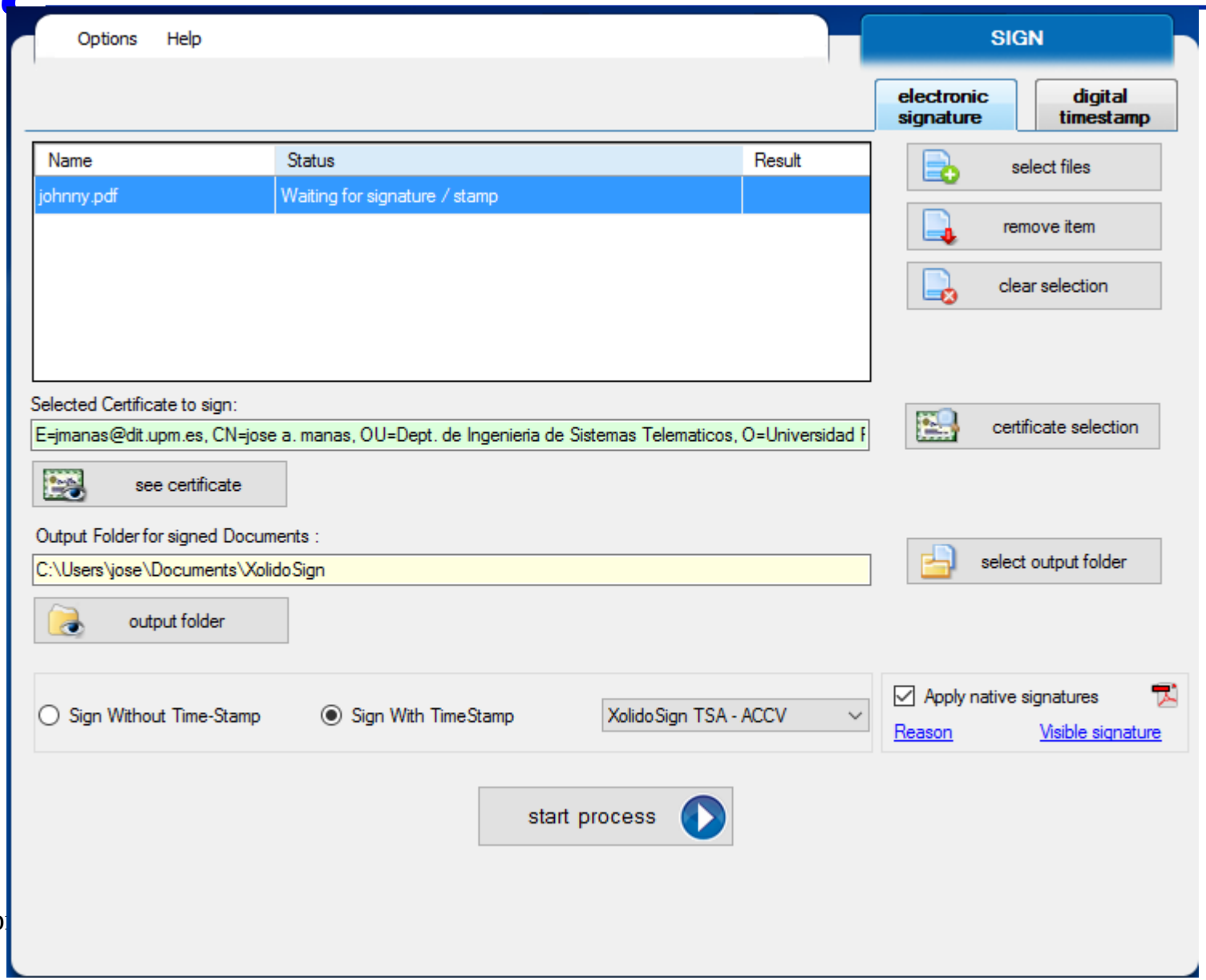
sello de tiempo en acrobat

- Edición > Preferencias > Seguridad
  - Servidores de marca de hora



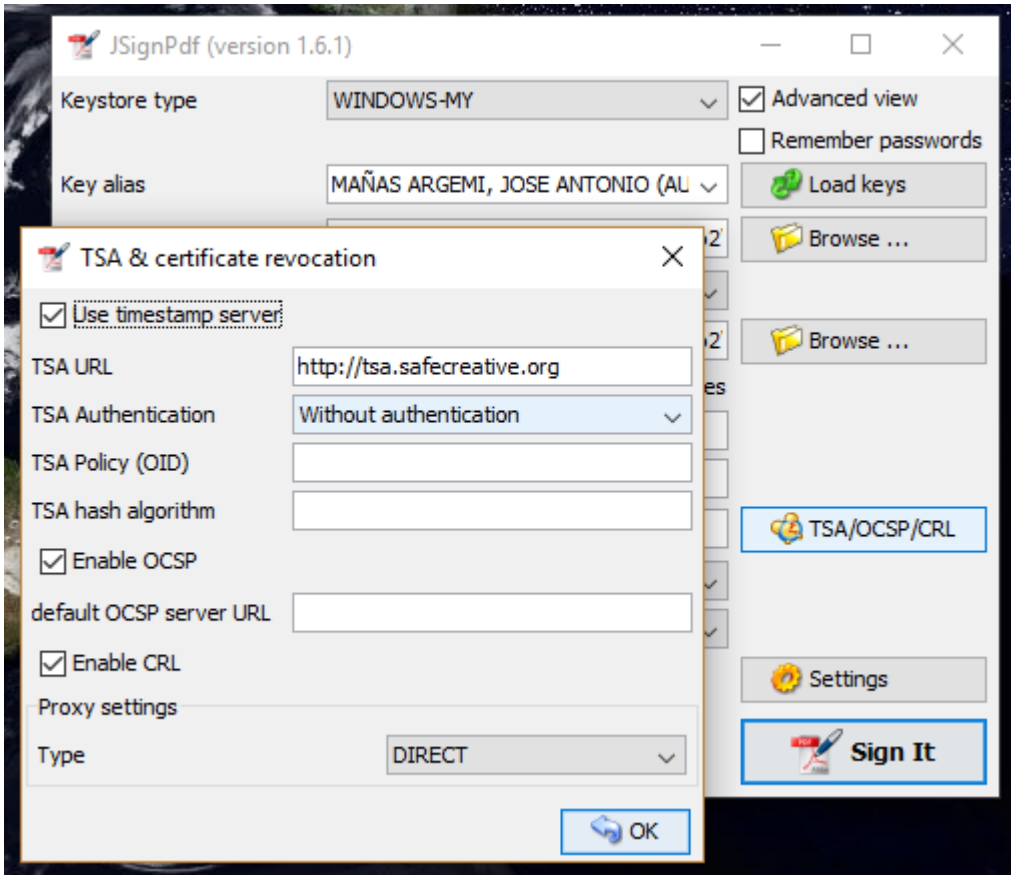


sello de tiempo Xolido



sello de tiempo jSignPdf

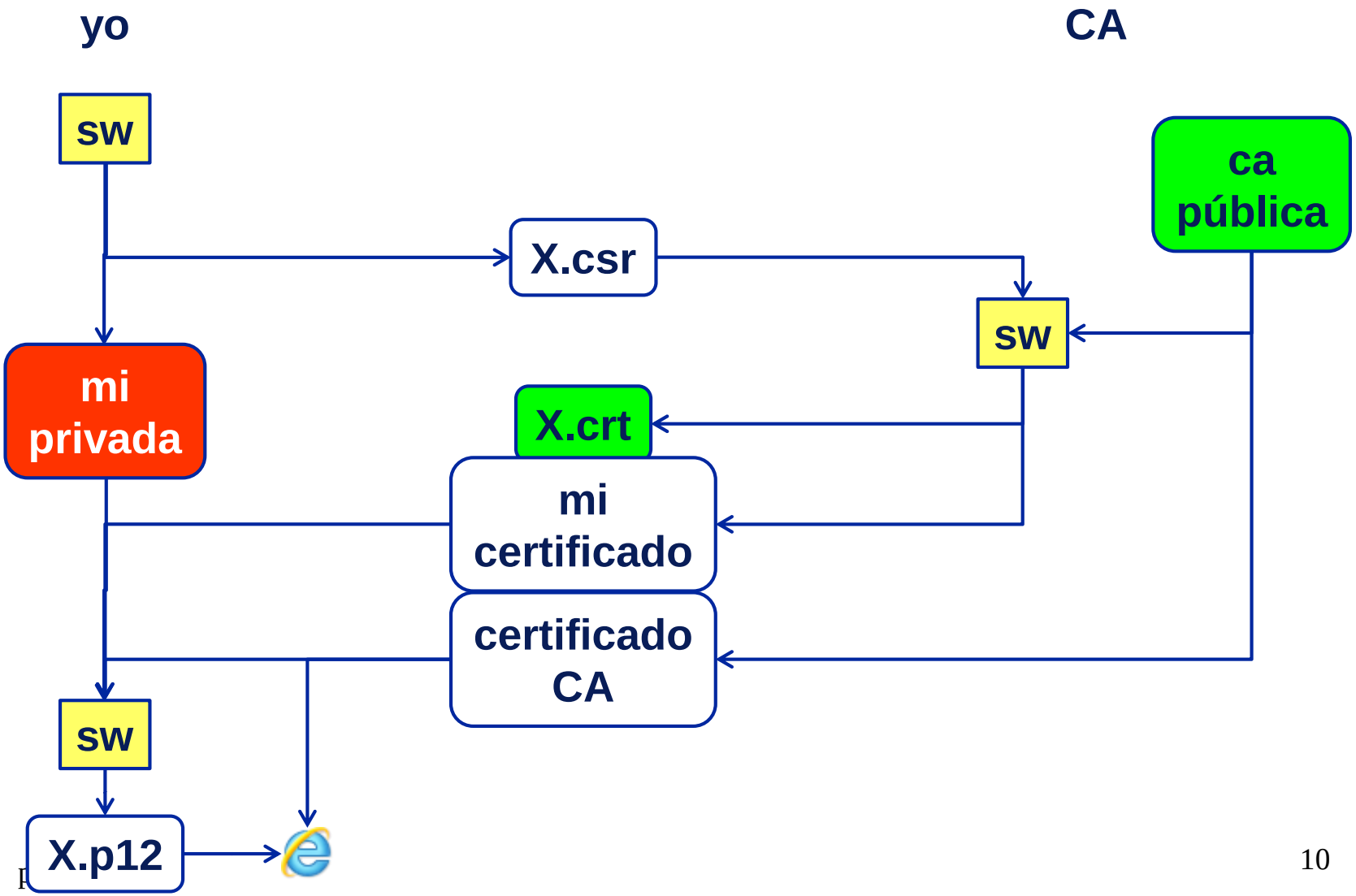
- Advanced view
  - TSA/OCSP/CRL



claves certificadas

1. genero mis claves
2. firmo mis claves demostrar mi propiedad (PoP)
3. mando una solicitud de certificación (CSR) a una CA
4. la autoridad de certificación (CA) firma mi certificado
   y me lo manda
5. uso mis claves y mi certificado para firmar mis documentos

pasos y ficheros



DNIe

preparación

1. En punto de expedición
   1. El chip genera y guarda mis claves
   2. la petición se genera y se firma dentro del chip
2. En el CPD de la policía
   1. se genera y se firma el certificado
3. El certificado se guarda en el chip

uso

1. Se prepara el hash de los datos
2. Se envía el hash al chip
3. El chip firma y devuelve la firma
4. Se adjunta la firma a los datos

DNI electrónico

- Se necesita DNI electrónico
  - driver
    - http://www.dnielectronico.es/descargas/
  - con los certificados válidos (actualizados)
    - http://www.dnielectronico.es/como_utilizar_el_dnie/verificar.html
  - lector de tarjetas
    - https://www.c3po.es/dni-electronico-dnie/
    - http://www.lectordni.com/
- Enlaces
  - http://www.dnielectronico.es/
  - http://www.usatudni.es/dnie/

certificado por una CA

preparación

1. En el navegador
    1. El navegador genera y guarda mis claves
    2. la petición se genera y se firma dentro del navegador
2. En el servidor de la CA
    1. se genera y se firma el certificado
3. El certificado se guarda en el registro

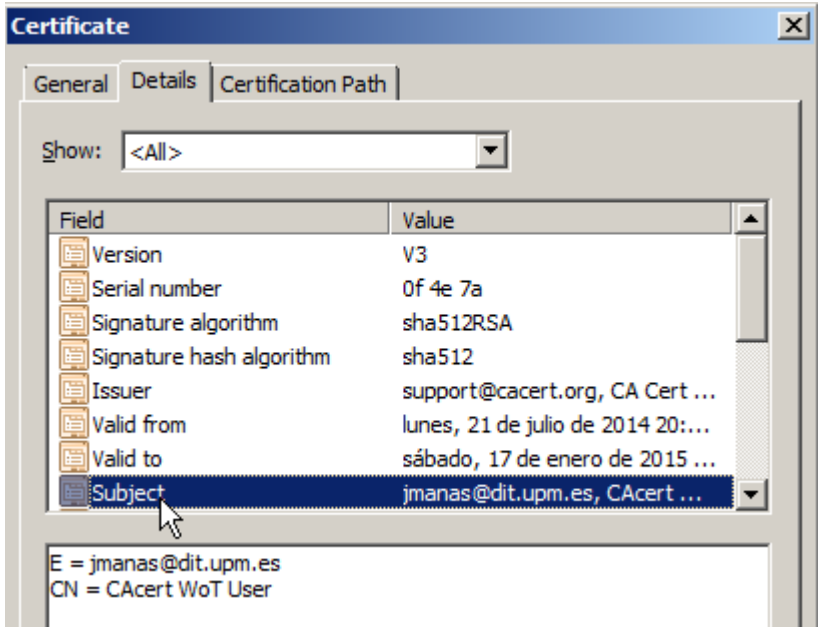
uso

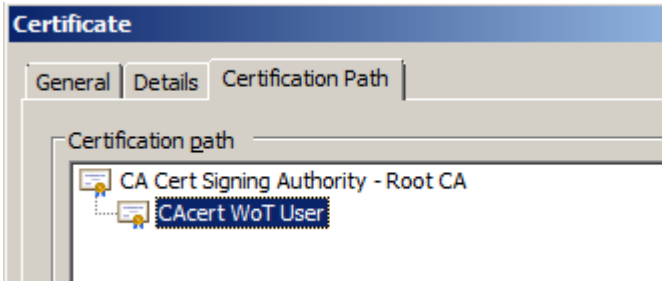
1. Se prepara el hash de los datos
2. El S.O. firma y devuelve la firma
3. Se adjunta la firma a los datos

certificado por una CA

http://www.cacert.org/

- http://wiki.cacert.org/Technology/KnowledgeBase/ClientCerts#To_get_your_client_cert_from_CAcert
- el certificado del profesor
  - http://www.dit.upm.es/~pepe/doc/seg4/cacert/jmanas.cer





OpenSSL

- Los profesores hemos preparado una CA miniatura
  - hemos usado OpenSSL
- Los alumnos pueden solicitar certificados que firmaremos con nuestra CA
- Pasos (OpenSSL)
  1. generar la pareja de claves
  2. generar una solicitud pkcs-10 (.csr)
  3. enviar la solicitud a jmanas@dit.upm.es
  4. recibirá como respuesta un certificado
  5. necesitará el certificado de la autoridad
  6. lo puede cargar en firefox, thunderbird, internet explorer, …

dit

autoridades de fechado gratuitas

free timestamp servers

http://www.sinadura.net/es/wik/-/wiki/sinadura/TSAServers

- http://tss.accv.es:8318/tsa
- http://ocsp.izenpe.com:8093
- http://tsa.starfieldtech.com/
- http://tsa.safecreative.org