

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

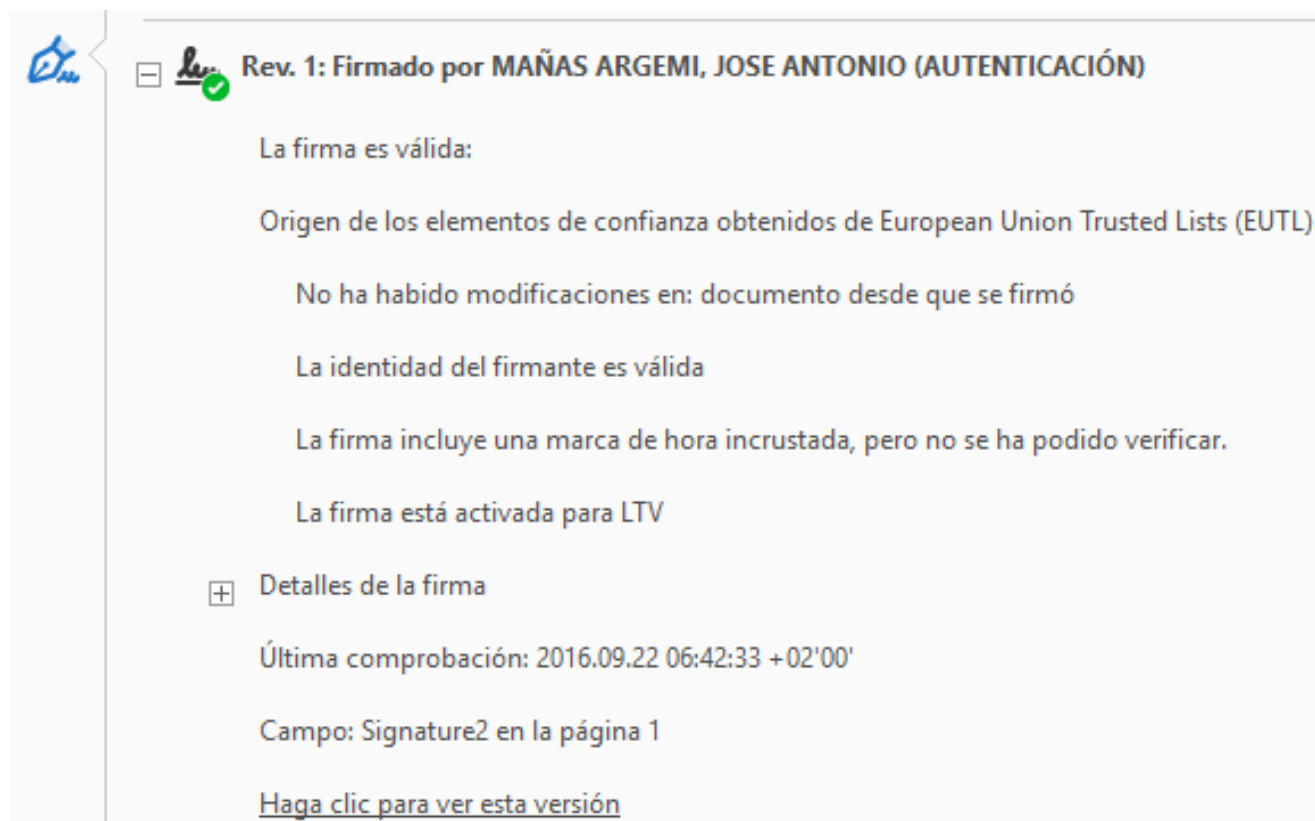
18 de septiembre de 2016

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

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

- 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

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



The screenshot displays a digital signature verification interface. At the top, a blue icon of a document with a checkmark is visible. Below it, a green checkmark icon is next to the text "Rev. 1: Firmado por MAÑAS ARGEMI, JOSE ANTONIO (AUTENTICACIÓN)". The main content area lists several verification details:

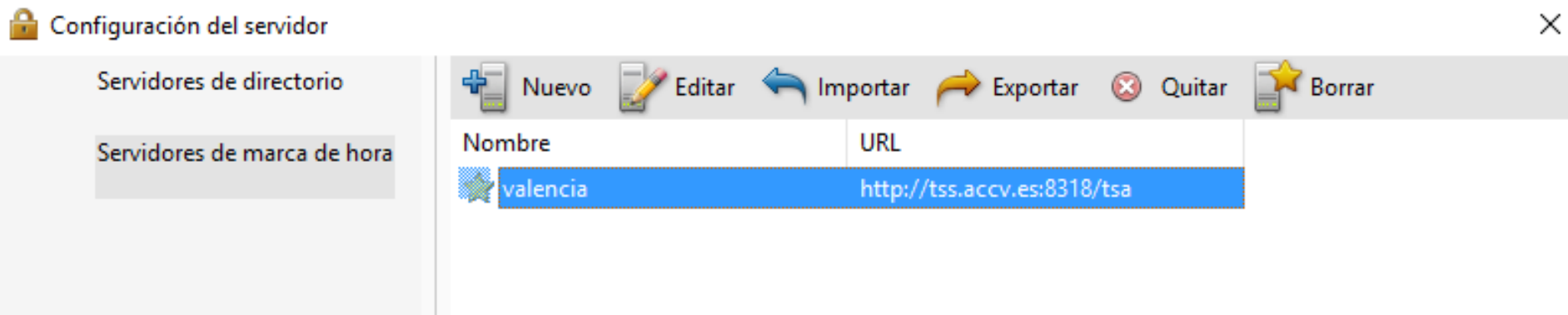
- La firma es válida:
- Origen de los elementos de confianza obtenidos de European Union Trusted Lists (EUTL).
- No ha habido modificaciones en: documento desde que se firmó
- La identidad del firmante es válida
- La firma incluye una marca de hora incrustada, pero no se ha podido verificar.
- La firma está activada para LTV

Below these details, there is a section titled "Detalles de la firma" with a plus icon. This section contains the following information:

- Última comprobación: 2016.09.22 06:42:33 +02'00'
- Campo: Signature2 en la página 1
- [Haga clic para ver esta versión](#)

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

Más...



sello de tiempo Xolido

Options Help

SIGN

electronic signature digital timestamp

Name	Status	Result
johnny.pdf	Waiting for signature / stamp	

Selected Certificate to sign:
E=jmanas@dit.upm.es, CN=jose a. manas, OU=Dept. de Ingenieria de Sistemas Telematicos, O=Universidad F

see certificate

Output Folder for signed Documents :
C:\Users\jose\Documents\Xolido Sign

output folder

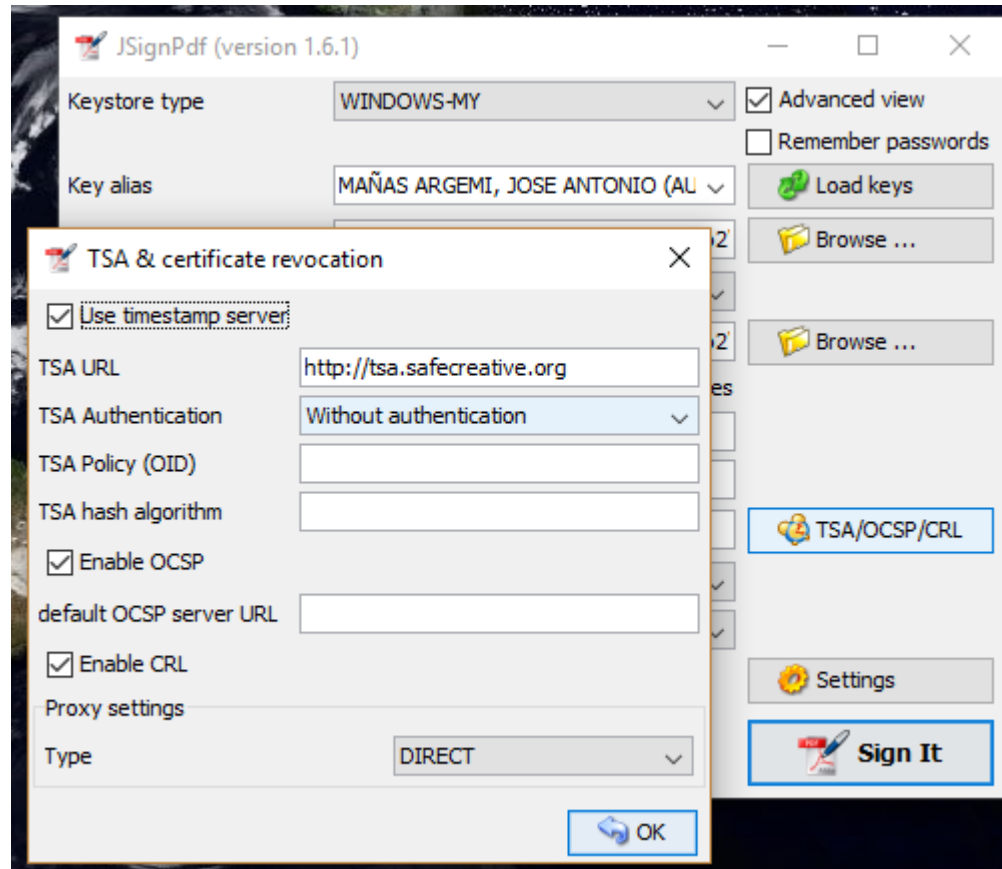
☐ Sign Without Time-Stamp ☒ Sign With TimeStamp XolidoSign TSA - ACCV

☒ Apply native signatures Reason Visible signature

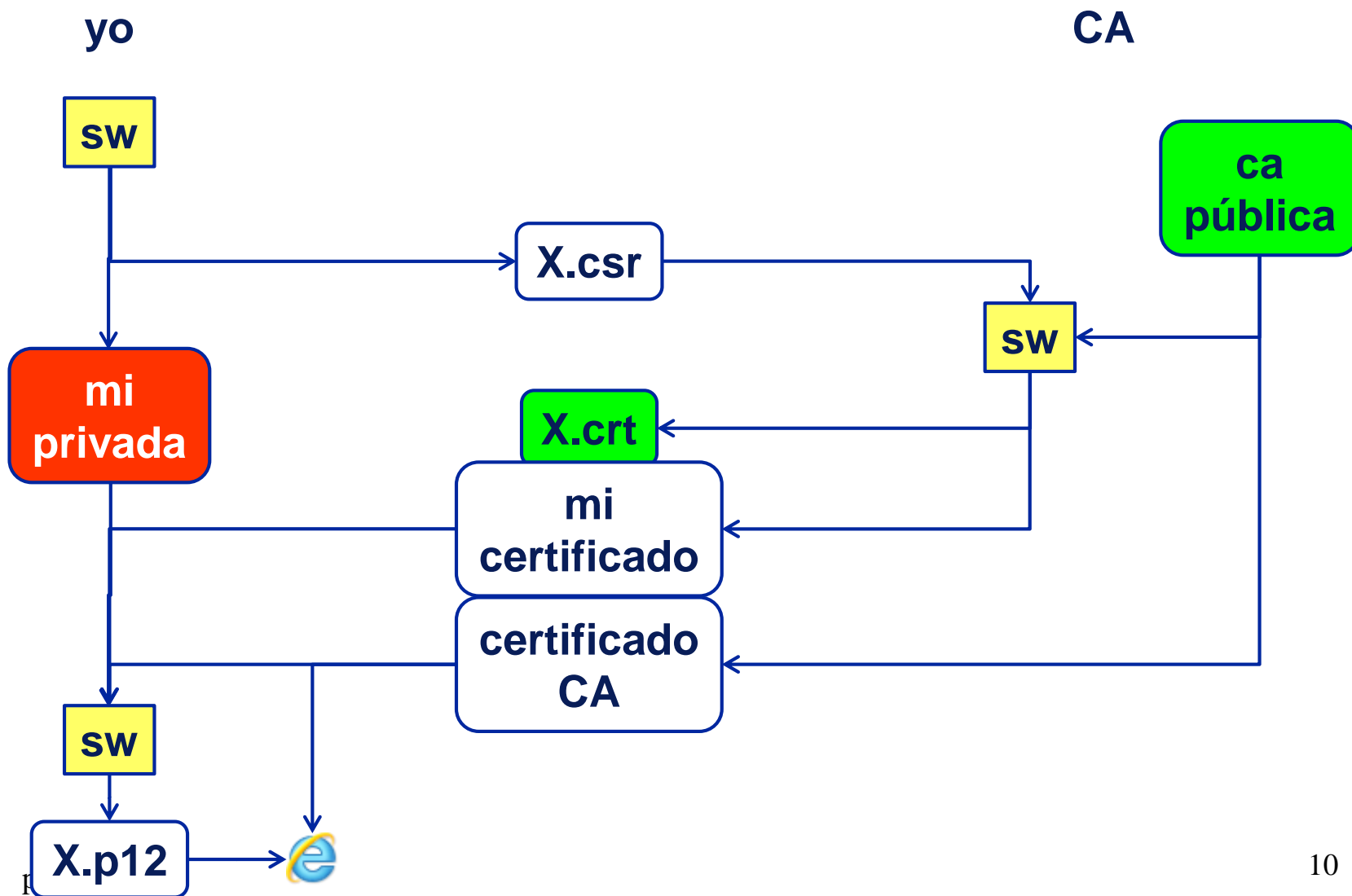
start process

select files
remove item
clear selection
certificate selection
select output folder

- Advanced view
 - TSA/OCSP/CRL



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



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

- 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/>

preparación

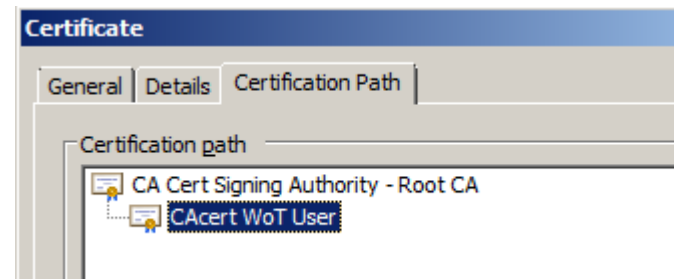
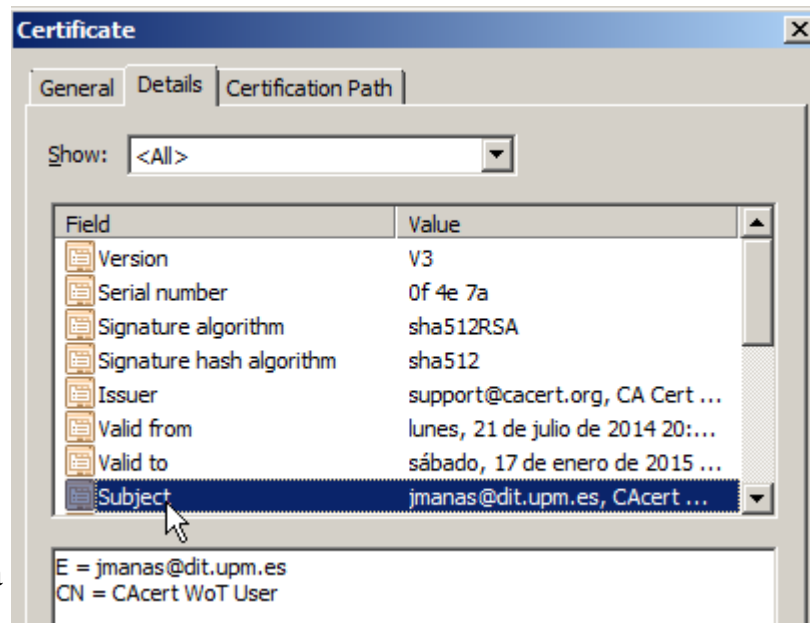
1. En el navegador
 1. El navegador genera y guarda mis claves
 2. la petición se genera y se firma dentro del navegador
2. En el servidor de la CA
 1. se genera y se firma el certificado
3. El certificado se guarda en el registro

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

<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>



- 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, ...

autoridades de fechado gratuitas

free timestamp servers

<http://www.sinadura.net/es/wik/-/wiki/sinadura/TSA Servers>

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