exercise 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

tasks

1. Sign a PDF document with one of …
   a) electronic identity card (DNIe)
   b) free digital certificate (CAcert)
   c) teachers' certification authority (CA)

PDF signing

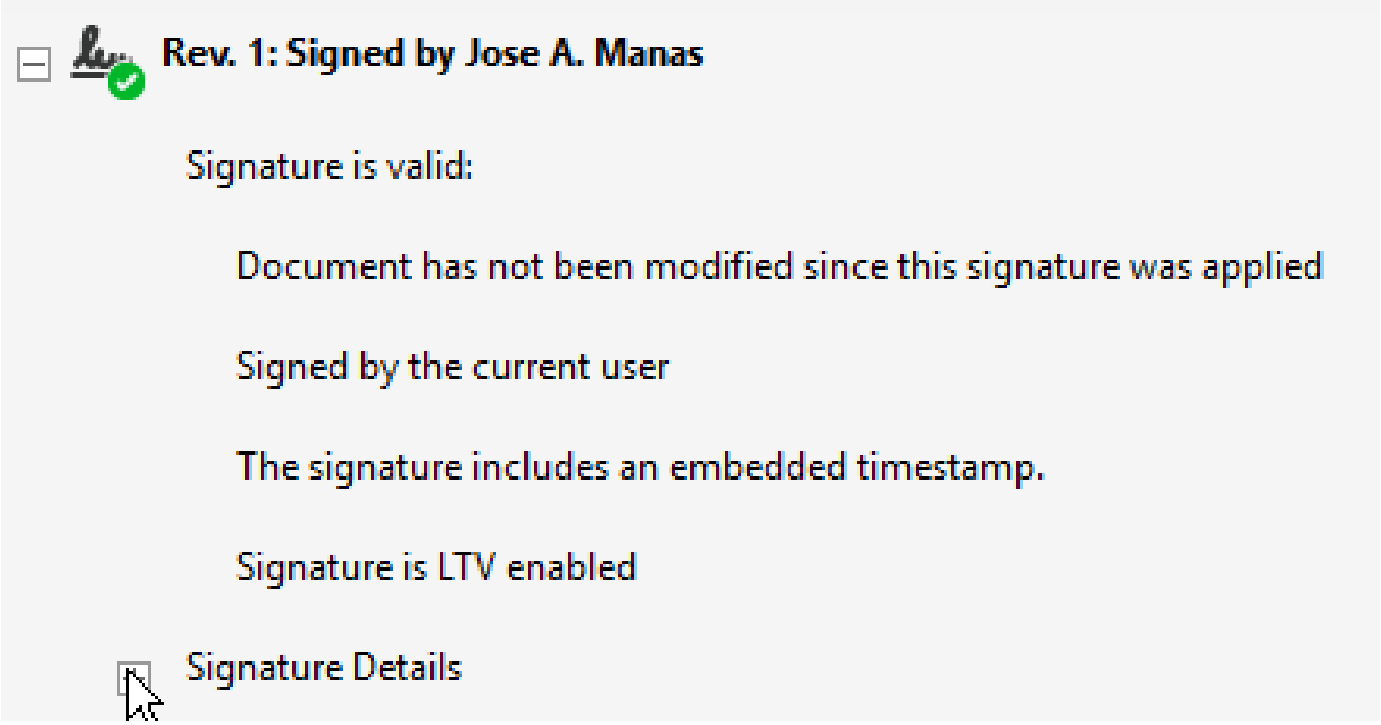
- Objective
  - using electronic signature to authenticate PDF documents
- Options: choose one (or more) of …
  a) DNIe – you need a DNIe and a card reader
  b) CAcert
  c) OpenSSL

PDF signing

- Software (options)
  - Adobe Acrobat Reader
  - Xolido -- http://www.en.xolido.com/lang/
    - Xolido Sign Desktop (free)
  - JSignPdf -- http://jsignpdf.sourceforge.net/
- Task
  1. Open a PDF doc
  2. Digitally sign, including a timestamp
  3. Send as an attachment to the teacher jmanas@dit.upm.es

signature

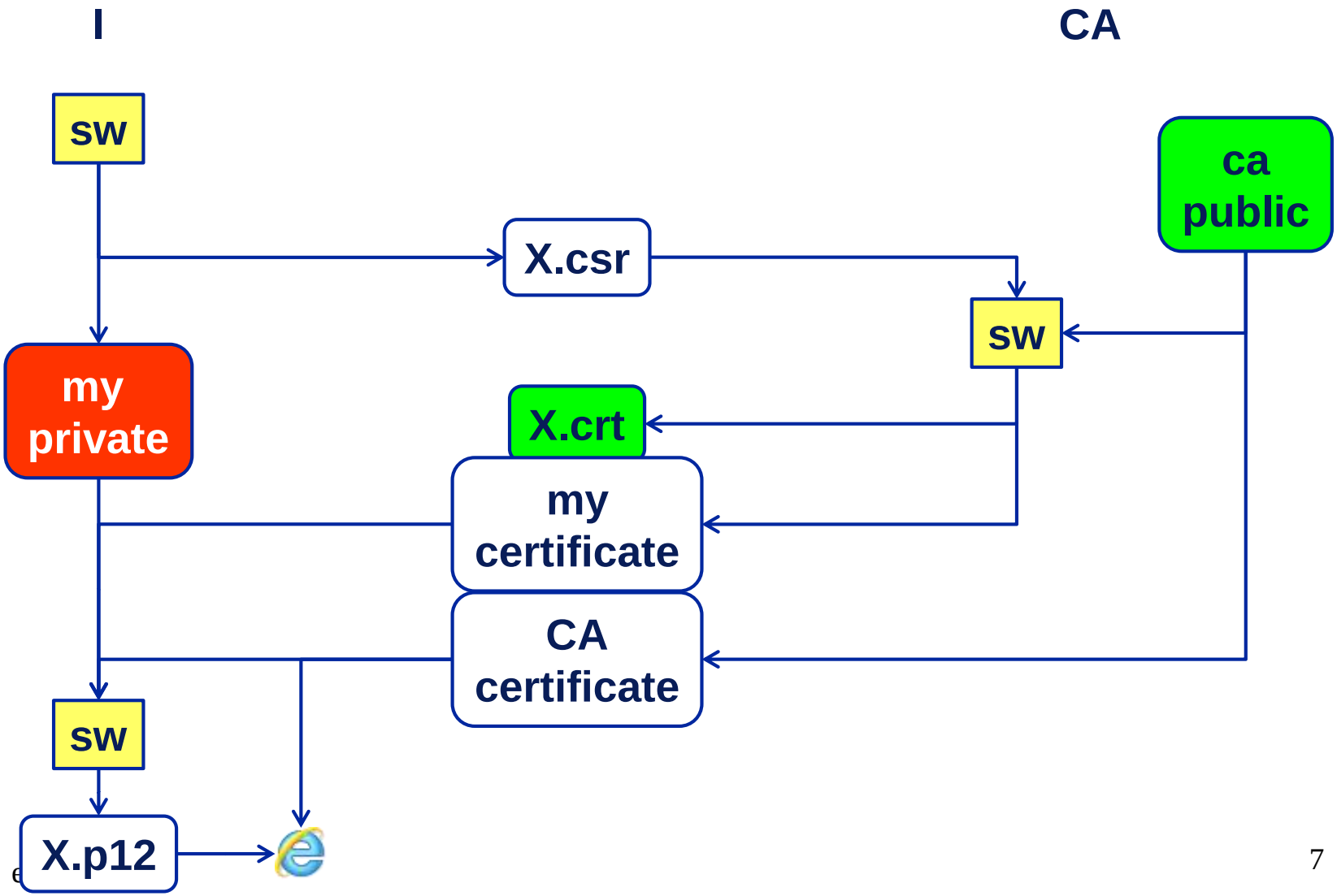
- Not required, but it is recommended to produce a LTV signature
- A timestamp is required



certified keys

1. I generate my keys
2. I sign my own keys (proof of posession)
3. I send a certificate signing request (csr) to an authority (CA)
4. the certification authority signs my certificate
   and returns it to me
5. I use my keys and my certificate to sign my documents

steps & files


I
CA
sw
ca
public
X.csr
sw
my
private
X.crt
my
certificate
CA
certificate
sw
X.p12

DNIe

preparatory activities

1. At the issue point
    1. the chip generates and saves my keys
    2. the csr is generated and signed in the chip
2. At police data center
    1. the certificate is generated and signed
3. The certificate is stored in the chip

usage

1. Acrobat prepares a hash
2. The hash is send to the chip
3. The chip signs and returns signature
4. Signature is saved in PDF

electronic DNI

- You need a smart card
  - driver
    - http://www.dnielectronico.es/descargas/
  - with up-to-date certificates
    - http://www.dnielectronico.es/como_utilizar_el_dnie/verificar.html
  - card reader
    - https://www.c3po.es/dni-electronico-dnie/
    - http://www.lectordni.com/
- Links
  - http://www.dnielectronico.es/
  - http://www.usatudni.es/dnie/

certified by a CA

preparatory activities

1. In the browser
    1. the browser generates and saves keys
    2. the csr is generated and signed in the browser
2. At CA data center
    1. the certificate is generated and signed
3. Certificate is saved in registry

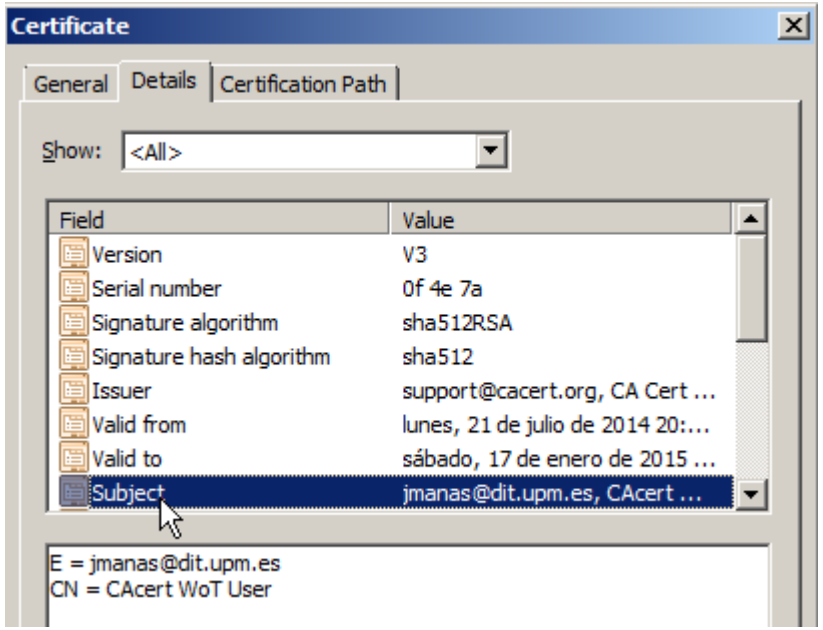
usage

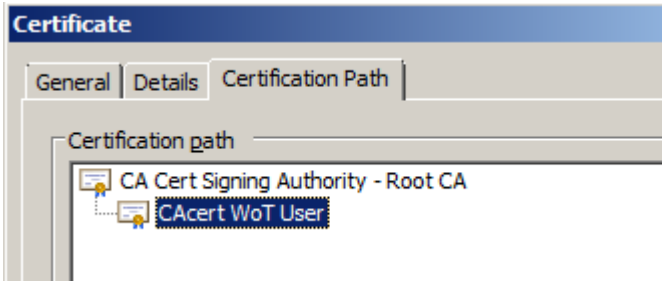
1. Prepare data hash
2. O.S. signes
3. Signature is saved along data

certified by a CA

http://www.cacert.org/

- http://wiki.cacert.org/Technology/KnowledgeBase/ClientCerts#To_get_your_client_cert_from_CAcert
- teacher's
  - http://www.dit.upm.es/~pepe/doc/seg4/cacert/jmanas.cer





OpenSSL

- Teachers have prepared a tiny CA
  - using OpenSSL
- Students may request certificates
  we will sign with our CA
- Steps (OpenSSL)
  1. generate key pair
  2. generate a request (csr, pkcs-10)
  3. send request to manas@dit.upm.es
  4. the cert will be returned to you
  5. load your cert and CA's cert onto registry, browser(s), …

dit

timestamp authorities

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