
Linux Week 2012

Firma digital de documentos en Linux

Pablo Fonseca
Dirección de Informática Académica
PUCP

¿Para qué sirve?

- **Hacer trámites** del gobierno por internet.
 - **Firmar contratos.**
 - **Aprobar documentos**
 - Planos de ingeniería.
 - Presupuestos.
 - Autorizaciones.
-

Firma digital: ¿Qué se puede lograr?

- Garantizar **la identidad del que firma.**
 - Garantizar **la integridad del documento.**
-

¿Válido legalmente?

LEY Nº 27269

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

**LEY DE FIRMAS Y CERTIFICADOS
DIGITALES**

2000

*"(...) **RENIEC** inauguró hoy en San Isidro la primera oficina de la Entidad de Registro Digital del Estado Peruano (EREP) "*

24 de febrero del 2012

[http://www.reniec.gob.pe/portal/detalleNota.htm?
nota=551](http://www.reniec.gob.pe/portal/detalleNota.htm?nota=551)

2012

Certificados digitales: ¿Confianza?

DELEGACIÓN DE CONFIANZA: Un usuario confía en la validez de una firma digital **si confía en la autoridad certificadora (CA) que emitió el certificado.**

En PERÚ

- RENIEC inauguró una **autoridad certificadora** en Febrero 2012.
 - Para personas naturales: **DNI Electrónico.**
-

Firmando: lo que debemos saber (I)

- Un documento se firma con un **certificado digital**.
 - Los certificados digitales se guardan en **contenedores**.
-

Firmando: lo que debemos saber (II)

- Un documento PDF puede tener **varias firmas digitales.**
 - Las firmas pueden ser validadas por una **Autoridad de Sello de Tiempo (TSA).**
-

Tipos de firma digital

- **Asistida**

- ¿Quién lo usa? : Usuarios que aprueban documentos, firman contratos, etc.

- **Silenciosa**

- ¿Quién lo usa? : Aplicaciones web, firmado en batch, etc.

Contenedores: ¿Dónde guardo los certificados?

- PKCS #12 (*.p12 *.pfx)
 - Java Key Store (JKS)
 - WINDOWS-MY
 - Otros
-

JSignPDF: Características

- Open source (MPL, LGPL).
 - Firmas visibles.
 - Estampa de tiempo.
 - Validación CRL, OCSP
 - Configuración del nivel de certificación
 - Encriptación de PDF y derechos de acceso.
 - Procesamiento en batch.
-

JSignPDF vs Software Comercial

- Las funcionalidades más importantes están soportadas.
 - Costo por licencia: \$ 0.00 vs 1000'\$
 - Código fuente disponible.
 - Licencia permite desarrollar software comercial.
 - Funciona como plugin para OpenOffice / LibreOffice.
-

Creando certificados de prueba

- **Crear root certificate**
 - `/etc/pki/tls/misc/CA -newca`
 - **Crear certificado**
 - `/etc/pki/tls/misc/CA -newreq`
 - `/etc/pki/tls/misc/CA -sign`
 - **Convertir PEM en x509 para usar el certificado en un Keystore**
 - `openssl x509 -in /path/cacert.pem -out root_certificate.ca`
 - **Convertir a pfx**
 - `openssl pkcs12 -inkey newkey.pem -in newcert.pem -export -out user_certificate.pfx`
 - **Importar certificado en JKS**
 - `keytool -importcert -file /path/root_certificate.ca -keystore keystore.jks`
-

Crear root certificate

/etc/pki/tls/misc/CA -newca

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    f3:f3:cf:4e:e2:f4:f7:1f
  Validity
    Not Before: Mar 13 14:59:06 2012 GMT
    Not After : Mar 13 14:59:06 2015 GMT
  Subject:
    countryName           = PE
    stateOrProvinceName  = Lima
    organizationName     = Palefo
    organizationalUnitName = Technology
    commonName           = Palefo
    emailAddress         = pfonseca@pucp.edu.pe
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D0
    X509v3 Authority Key Identifier:
      keyid:D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D0

0

    X509v3 Basic Constraints:
      CA:TRUE
Certificate is to be certified until Mar 13 14:59:06 2015 GMT (1095 days)

Write out database with 1 new entries
```

Crear un certificado (I)

```
/etc/pki/tls/misc/CA -newreq
```

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:PE
State or Province Name (full name) []:Lima
Locality Name (eg, city) [Default City]:Lima
Organization Name (eg, company) [Default Company Ltd]:Palefo
Organizational Unit Name (eg, section) []:Technology
Common Name (eg, your name or your server's hostname) []:Pablo Fonseca
Email Address []:user@server.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
```

Crear un certificado (II)

```
/etc/pki/tls/misc/CA -sign
```

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    f3:f3:cf:4e:e2:f4:f7:20
  Validity
    Not Before: Mar 13 15:15:07 2012 GMT
    Not After : Mar 13 15:15:07 2013 GMT
  Subject:
    countryName           = PE
    stateOrProvinceName   = Lima
    localityName          = Lima
    organizationName      = Palefo
    organizationalUnitName = Technology
    commonName            = Pablo Fonseca
    emailAddress          = user@server.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      25:06:E6:59:34:2D:42:8C:C3:82:E6:9A:9D:DC:38:1E:35:2E:61:07
    X509v3 Authority Key Identifier:
      keyid:D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D0

Certificate is to be certified until Mar 13 15:15:07 2013 GMT (365 days)
Sign the certificate? [y/n]:y
```

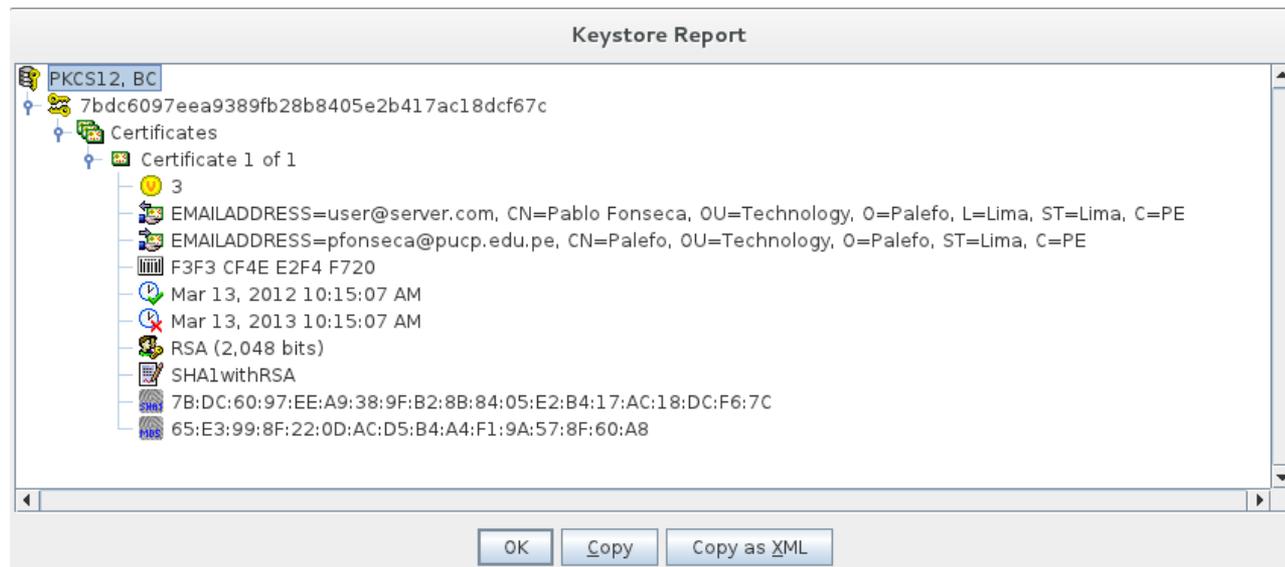
```
1 out of 1 certificate requests certified, commit? [y/n]y
```

Exportar un certificado a PFX

```
openssl pkcs12 -inkey newkey.pem -in newcert.pem -export -out  
user_certificate.pfx
```

```
Enter pass phrase for newkey.pem:  
Enter Export Password:  
Verifying - Enter Export Password:
```

Se necesitará usar el "Export Password" para poder usar el certificado.



Exportar el root certificate

```
openssl x509 -in cacert.pem -out root_certificate.cer
```

Firmar el PDF (I)

JSignPdf (version 1.3.0)

Keystore <u>t</u> ype	<input type="text" value="PKCS12"/>	<input checked="" type="checkbox"/> <u>A</u> dvanced view
<u>K</u> eystore file	<input type="text" value="xweek/certificados/user_certificate.pfx"/>	<input type="button" value="Browse ..."/>
Keystore <u>p</u> assword	<input type="text" value="****"/>	<input checked="" type="checkbox"/> <u>R</u> emember passwords
Key <u>a</u> lias	<input type="text" value="1"/>	<input type="button" value="Load keys"/>
Key <u>p</u> ass <u>w</u> ord	<input type="text"/>	
<u>I</u> nput PDF file	<input type="text" value="/nfonseca/Downloads/cv_nfonseca.pdf"/>	<input type="button" value="Browse ..."/>
	<input type="checkbox"/> <u>E</u> ncrypted	
<u>O</u> utput PDF file (optional)	<input type="text"/>	<input type="button" value="Browse ..."/>
	<input type="checkbox"/> <u>A</u> ppend signature to the existing ones	
<u>R</u> eason (optional)	<input type="text" value="CV Actualizado v aprobado"/>	
<u>L</u> ocation (optional)	<input type="text" value="PUICP. Lima"/>	
<u>C</u> ontact (optional)	<input type="text"/>	<input type="button" value="TSA/OCSP/CRL"/>
<u>C</u> ertification level	<input type="text" value="Form filling and annotations allowed"/>	
<u>H</u> ash algorithm	<input type="text" value="SHA256"/>	
	<input checked="" type="checkbox"/> <u>V</u> isible signature	<input type="button" value="Settings"/>
		<input type="button" value="Sign It"/>

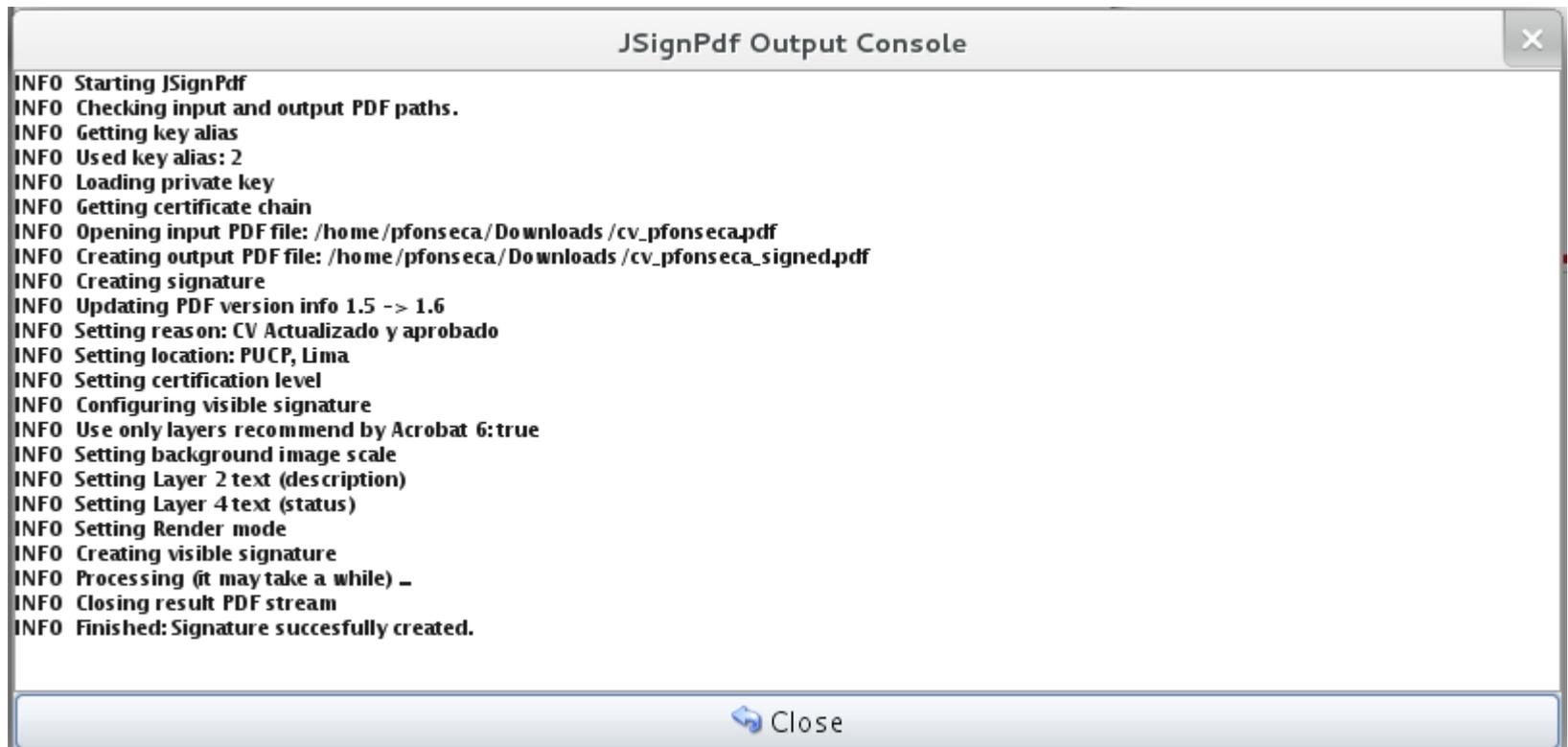
Firmar el PDF (II)

Seleccionar el área donde se firmará.

Preview/Select

PABLO FONSECA
Mobile. +51-956470916 Office +51-1-6262000 Ext. 3774
<http://metis.pucp.edu.pe/~plonseca>
plonseca@pucp.edu.pe

Firmar el PDF (III)



```
JSigPdf Output Console
INFO Starting JSigPdf
INFO Checking input and output PDF paths.
INFO Getting key alias
INFO Used key alias: 2
INFO Loading private key
INFO Getting certificate chain
INFO Opening input PDF file: /home/pfonseca/Downloads/cv_pfonseca.pdf
INFO Creating output PDF file: /home/pfonseca/Downloads/cv_pfonseca_signed.pdf
INFO Creating signature
INFO Updating PDF version info 1.5 -> 1.6
INFO Setting reason: CV Actualizado y aprobado
INFO Setting location: PUCP, Lima
INFO Setting certification level
INFO Configuring visible signature
INFO Use only layers recommend by Acrobat 6:true
INFO Setting background image scale
INFO Setting Layer 2 text (description)
INFO Setting Layer 4 text (status)
INFO Setting Render mode
INFO Creating visible signature
INFO Processing (it may take a while) _
INFO Closing result PDF stream
INFO Finished: Signature succesfully created.
```

Close

Firmar el PDF (IV)

The screenshot displays the Adobe Reader interface for a document titled "cv_pfonseca_signed.pdf". The menu bar includes "File", "Edit", "View", "Document", "Tools", "Window", and "Help". The toolbar shows various icons for printing, navigation, and search, with the current page being 1 of 2 and a zoom level of 71.7%. A status bar at the top indicates the document is "Certified by Pablo Fonseca <user@server.com>, Palefo, certificate issued by Palefo." and includes a "Signature Panel" button. On the left, the "Signatures" panel is open, showing a "Validate All" button and a list of signatures, including one by Pablo Fonseca. The main content area displays the following text:

Digitally signed by Pablo Fonseca
Date: 2012.03.13 10:40:28 PET

PABLO FONSECA
Mobile. +51-956470916 Office +51-1-6262000 Ext. 3774
<http://matix.pucp.edu.pe/~pfonseca>

Siguiente paso:

- Usar JSignPDF como librería.
 - Usar JSignPDF para firma en batch.
-

Conclusiones

- Momento ideal en el Perú para desarrollar software que incluya posibilidad de firma digital.
 - JSignPDF es muy completo y se podría usar como librería o como aplicación.
-

Referencias útiles

- **RENIEC:** <http://www.reniec.gob.pe/portal/principalPKI.htm>
 - **JSIGNPDF:**
<http://jsignpdf.sourceforge.net/>
-

¿Preguntas?

Gracias!

Contacto:

Pablo Fonseca

Email: pfonseca@pucp.edu.pe

Twitter: [@palefo](https://twitter.com/palefo)
