

Guía para solicitar certificados de persona jurídica en Linux

Este documento permite al lector conocer los pasos necesarios para solicitar los certificados para personas jurídicas en sistemas operativos Linux

Contenido

Parte 1: Modificar el archivo de configuración de openssl.....	2
Parte 2: Generar el REQ para Sello Electrónico.....	4
Parte 3: Generar el REQ para Agente Electrónico.....	6
Parte 4: Visualizando los requests generados (Opcional).	9
Parte 5: Anexos.....	10

La presente guía documenta los pasos a seguir para realizar una solicitud de certificados digitales para una persona jurídica, utilizando el sistema operativo Linux en una distribución basada en "Debian" o similares.

Nota: Los pasos descritos en esta guía fueron probados en el sistema operativo Ubuntu versión 12.04 LTS.

Parte 1: Modificar el archivo de configuración de openssl.

- 1) Localice el archivo **openssl.cnf**. Habitualmente se encuentra en el directorio **/etc/ssl/**.
- 2) Haga una copia de respaldo del archivo con el comando:

cp openssl.cnf openssl.cnf.original

- 3) Abra el archivo "openssl.cnf" con su editor de texto preferido.
- 4) Busque las líneas mostradas en la imagen, bajo la cabecera: **[v3_req]** y colocar los siguientes parámetros bajo ella:
 - Para un request de Sello Electrónico: **keyUsage = digitalSignature, nonRepudiation**

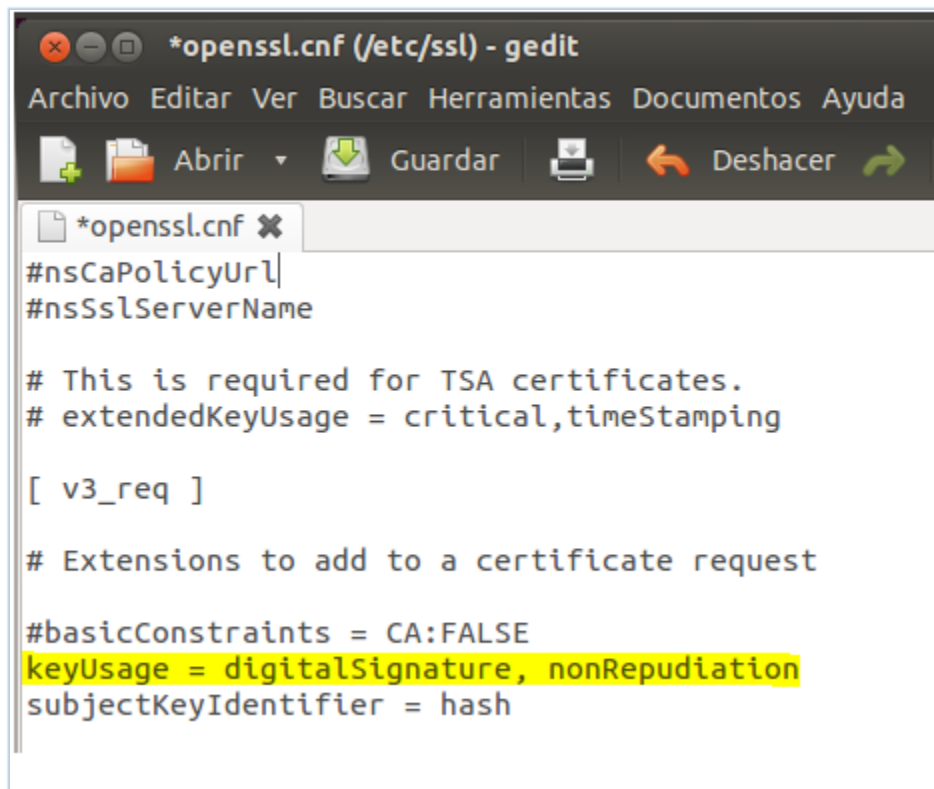
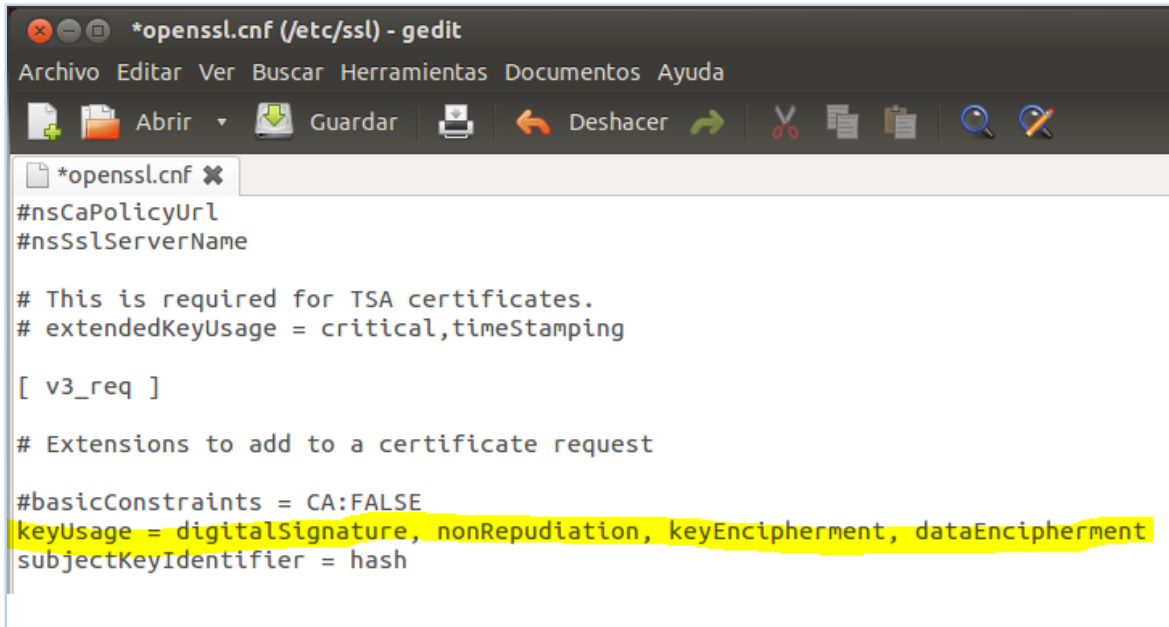


Imagen 1

- Para un request de Agente Electrónico:

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, DataEncipherment



```
*openssl.cnf (/etc/ssl) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*openssl.cnf X
#nsCaPolicyUrl
#nsSslServerName

# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping

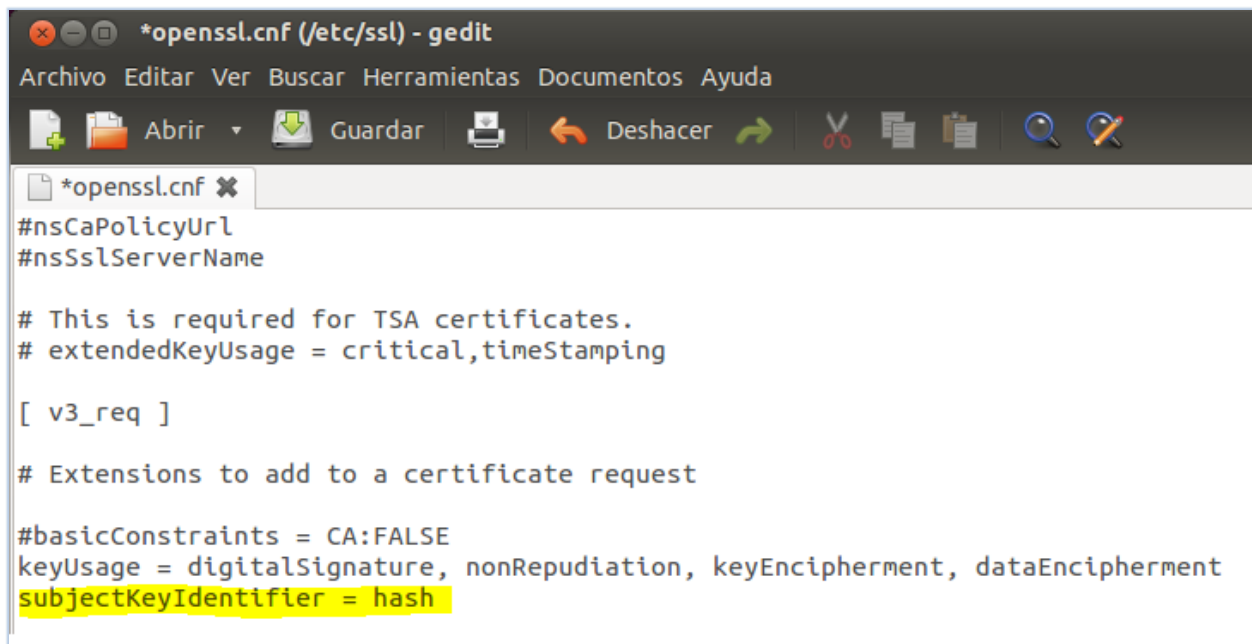
[ v3_req ]

# Extensions to add to a certificate request

#basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectKeyIdentifier = hash
```

Imagen 2

- Para un request de Sello o Agente Electrónico: **subjectKeyIdentifier = hash**



```
*openssl.cnf (/etc/ssl) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*openssl.cnf X
#nsCaPolicyUrl
#nsSslServerName

# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping

[ v3_req ]

# Extensions to add to a certificate request

#basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectKeyIdentifier = hash
```

Imagen 3

Si observa que estos ya están, pero antecidos con un símbolo "#", significa que están comentados. Remueva el símbolo de numeral. Si ya están, pero con diferente valor, proceda a modificarlos.

- 5) Se debe configurar el componente PKCS#11 del dispositivo criptográfico como un "engine" de openssl. En caso de que no tenga instalado el paquete *libengine-pkcs11-openssl*, debe instalarlo previamente. Primero debe ingresar a openssl digitando el siguiente comando en la terminal:

openssl

Una vez dentro de la terminal de openssl debe digitar el siguiente comando:

```
engine -t dynamic -pre SO_PATH:/usr/lib/engines/engine_pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/ruta/libreriaPKCS11.so
```

Donde el valor de MODULE_PATH debe reemplazarse por la ruta y archivo de la librería PKCS#11 del dispositivo criptográfico que tiene las llaves criptográficas que serán utilizadas para generar el request de certificado.

Salga de openssl digitando **exit**.

Parte 2: Generar el REQ para Sello Electrónico¹.

- 2.1 Obtenga la cédula jurídica y la razón social de su entidad utilizando el formulario de generación de certificado en el sitio de Central Directo:

Información para generar el request

Para generar el request de certificado, es necesario descargar el archivo .inf con la información de su empresa y completar los campos con las etiquetas delimitadas por los caracteres "{#" y "#}".

```
[Version]
Signature= "SWindows NTS"

[NewRequest]

Subject = "2.5.4.5=CPJ-4-000-004017,CN=BANCO CENTRAL DE COSTA RICA (SELLO ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 2048
RequestType = PKCS10
KeySpec = AT_SIGNATURE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE"
ProviderName = "{#PROVEEDOR CRIPTOGRAFICO#}"
ProviderType = "{#VALOR_TIPO_PROVEEDOR#}"
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE
```

Descargue el archivo .inf: [DatosPJSello.inf](#)

Para terminar de generar el request debe continuar con los pasos que se indican en la guía: [Guía para generar una solicitud o request](#)

Atrás Siguiente Cerrar

Imagen 4

- 2.2 Abra una terminal en el sistema operativo, como muestra la imagen 5.

¹ Las instrucciones de esta guía asumen que usted ya ha instalado y generado las llaves privadas de los certificados en un dispositivo seguro. Ver prerequisites para determinar si es seguro. Si no ha realizado estos procedimientos, consulte a su proveedor.

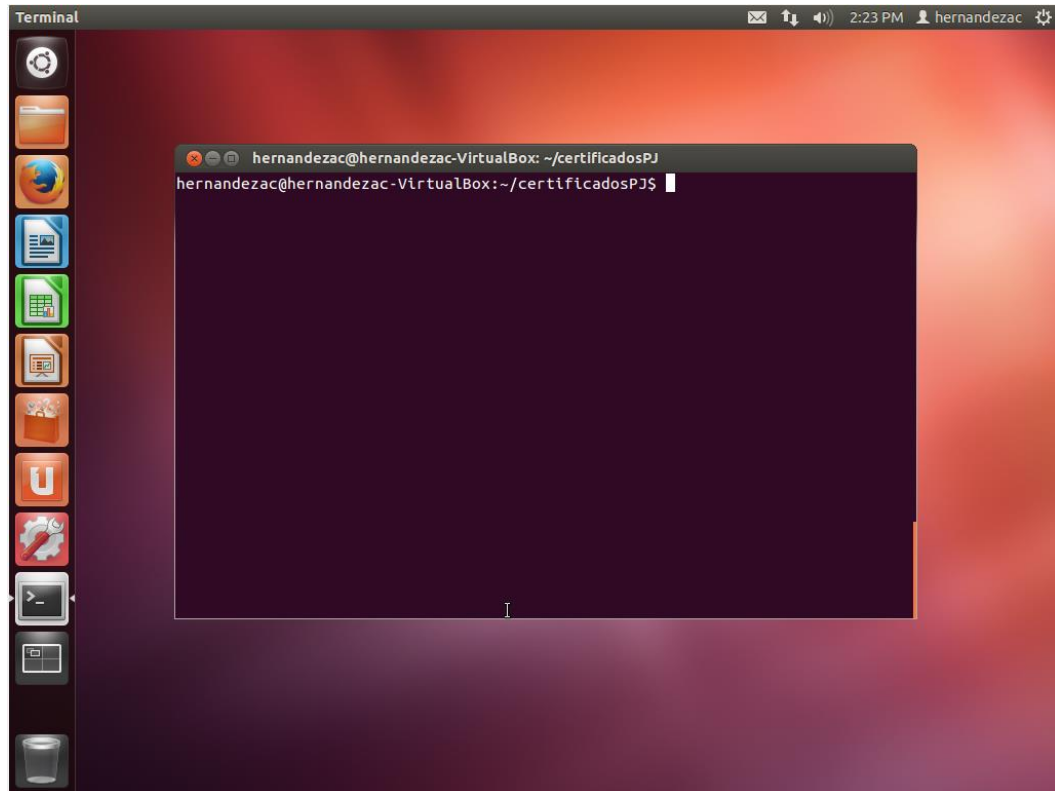


Imagen 5

2.3 Si desea generar un request, en la terminal que abrió en el apartado 2.2, ejecute el siguiente comando:

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5=CPJ-{#CEDULA JURIDICA#}/CN={#RAZON SOCIAL#} (SELLO ELECTRONICO)/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestSello.req
```

Donde la ***{#RAZON SOCIAL#}*** no debe superar los 44 caracteres para el caso de SELLO ELECTRÓNICO

Por ejemplo, para la entidad "**PRICOSE PRIMERA SOCIEDAD AGENCIA DE SEGUROS SOCIEDAD ANONIMA**" que supera los **44** caracteres en su razón social, con cedula jurídica: **3-101-184673** quedaría así.

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5= CPJ-3-101-184673/CN=PRICOSE PRIMERA SOCIEDAD AGENCIA DE SEGUROS (SELLO ELECTRONICO)/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestSello.req
```

2.4 Observe que en la instrucción hay etiquetas delimitadas por los caracteres "***{#}***" y "***#}***". **Estos son los únicos campos que usted debe modificar para realizar la solicitud de un certificado de sello electrónico de Persona Jurídica.** Cámbielos según se indica a continuación:

- **{#CEDULA JURIDICA#}**: Escriba aquí la cédula jurídica que se obtuvo en el paso 2.1. Por ejemplo, la cédula jurídica 3-101-123456 debe quedar como **CPJ-3-101-123456**.
- **{#RAZON SOCIAL#}**: Escriba aquí la razón social que se obtuvo en el paso 2.1.

Parte 3: Generar el REQ para Agente Electrónico

- 3.1 Obtenga la cédula jurídica y la razón social de su entidad utilizando el formulario de generación de certificado:

Información para generar el request

Para generar el request de certificado, es necesario descargar el archivo .inf con la información de su empresa y completar los campos con las etiquetas delimitadas por los caracteres "{#" y "#}".

```
[Version]
Signature= "$Windows NTS"

[NewRequest]
Subject = "2.5.4.5=CPJ-4-000-004017,CN=BANCO CENTRAL DE COSTA RICA (AGENTE ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 2048
RequestType = PKCS10
KeySpec = AT_KEYEXCHANGE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE | CERT_KEY_ENCIIPHERMENT_KEY_USAGE | CERT_DATA_ENCIIPHERMENT_KEY_USAGE"
ProviderName = "{#PROVEEDOR CRIPTOGRAFICO#}"
ProviderType = "{#VALOR_TIPO_PROVEEDOR#}"
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE

[RequestAttributes]
SAN = "{#DOMINIOS WEB#}"
```

Descargue el archivo .inf: [DatosPJAgente.inf](#)

Para terminar de generar el request debe continuar con los pasos que se indican en la guía: [Guía para generar una solicitud o request](#)

Atrás Siguiente Cerrar

Imagen 6

- 3.2 Si se requiere asegurar alguno de los dominios de Internet de su institución/compañía con este certificado, realice las siguientes instrucciones. Si no lo desea así, ejecute de inmediato el paso 3.3.
- Localice el archivo **openssl.cnf**. Habitualmente se encuentra en el directorio **/etc/ssl/**.
 - Haga una copia de respaldo del archivo con el comando:
 - cp openssl.conf openssl.conf.original**
 - Abra el archivo openssl.conf con su editor de texto preferido.
 - En la sección **[req]** del archivo, verifique que exista una línea que inicia con **req_extensions**. La misma no debe estar comentada.
 - El archivo debe verse como lo indica la imagen 7.

```
#####  
[ req ]  
default_bits          = 1024  
default_keyfile       = privkey.pem  
distinguished_name   = req_distinguished_name  
attributes            = req_attributes  
x509_extensions      = v3_ca # The extensions to add to the self signed cert  
req_extensions       = v3_req # The extensions to add to a certificate request
```

Imagen 7

- f. En el mismo archivo, ubíquese en la sección v3_req y asegúrese que incluye lo que se encuentra marcado en la imagen 8.

```
[ v3_req ]  
  
# Extensions to add to a certificate request  
  
#basicConstraints = CA:FALSE  
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment  
subjectKeyIdentifier = hash  
  
subjectAltName = @alt_names
```

Imagen 8

- g. Cree una nueva sección en el archivo, justo bajo la línea "subjectAltName=@alt_names" llamada **[alt_names]**. En esta sección se pueden incluir los nombres de los dominios con los que cuente la entidad, estos pueden ser de sitios o de servicios web que se deseen asegurar con el certificado de Agente Electrónico. Debe verificar que cumplan las siguientes reglas:

Para efectos prácticos vamos a suponer que una entidad cuenta con los dominios www.miempresa.co.cr, transacciones.miempresa.co.cr, mail.miempresa.co.cr, y *.miempresa.co.cr.

1. Se debe de escribir en minúscula.
2. Los dominios no pueden contener caracteres especiales como la tilde.
3. No debe contener http.
4. Se puede escribir un dominio o múltiples dominios
 - DNS.1 = [Host1].[DominioEntidad]
 - DNS.2 = [Host2].[DominioEntidad]
5. El número máximo de registros en el SAN es de 10 dominios.
6. Se puede escribir todo el dominio
 - DNS.1 = transacciones.miempresa.co.cr

Guía para solicitar certificados de persona jurídica en Linux

7. Se puede escribir sólo el final del dominio, pero debe tener un asterisco antes del primer punto

- DNS.1 = *.miempresa.co.cr

8. Los dominios deben encontrarse registrados a nombre de la entidad.

9. Debe incluirlos como se indica en la imagen 9:

```
subjectAltname = @alt_names
[alt_names]
DNS.1 = www.miempresa.co.cr
DNS.2 = transacciones.miempresa.co.cr
DNS.3 = mail.miempresa.co.cr
DNS.4 = *.miempresa.co.cr
```

Imagen 9

h. Guarde el archivo **openssl.cnf**.

3.3 En la misma terminal que abrió en el paso 1 de la Parte 2, ejecute el siguiente comando:

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5=CPJ-{#CEDULA JURIDICA#}/CN={#RAZON SOCIAL#} (AGENTE ELECTRONICO)/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestAgente.req
```

Donde la **{#RAZON SOCIAL#}** no debe superar los 43 caracteres para el caso de AGENTE ELECTRÓNICO

Por ejemplo, para entidad "**PRICOSE PRIMERA SOCIEDAD AGENCIA DE SEGUROS SOCIEDAD ANONIMA**" que supera los **43** caracteres en su razón social, con cédula jurídica: **3-101-184673** quedaría así.

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5=CPJ-3-101-184673/CN=PRICOSE PRIMERA SOCIEDAD AGENCIA DE SEGUROS (AGENTE ELECTRONICO)/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestAgente.req
```

Nota: Si no ha realizado la carga del "engine" de PKCS#11, como lo indica el paso 5 de la "Parte 1", debe ejecutar el comando para cargar el "engine".

3.4 Observe que en la instrucción hay etiquetas delimitadas por los caracteres "{#" y "#}". **Estos son los únicos campos que usted debe modificar para realizar la solicitud de un certificado de agente electrónico de Persona Jurídica.** Cámbielos según se indica a continuación:

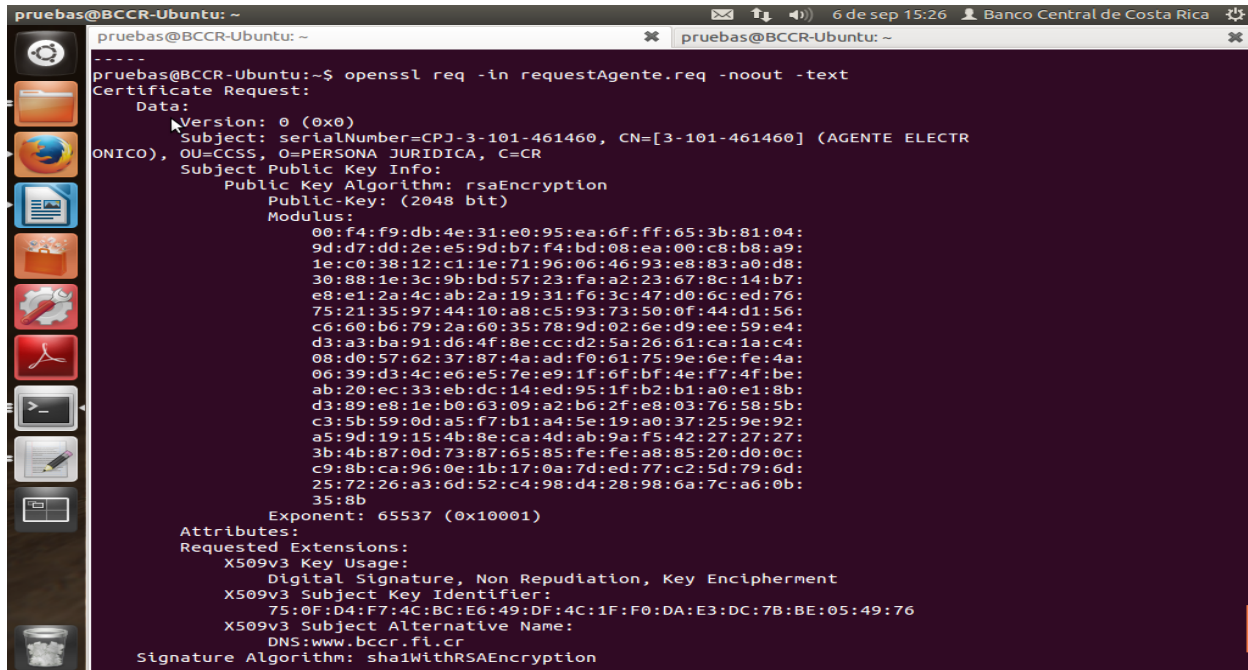
- **{#CEDULA JURIDICA#}**: Escriba aquí la cédula jurídica que se obtuvo en el paso 3.1. Por ejemplo, la cédula jurídica 3-101-123456 debe quedar como **CPJ-3-101-123456**.
- **{#RAZON SOCIAL#}**: Escriba aquí la razón social que se obtuvo en el paso 3.1.

Parte 4: Visualizando los requests generados (Opcional).

Si desea comprobar la estructura del .req generado es necesario abrir la ventana de comandos y colocarse en la ruta que está el archivo luego de esto es necesario colocar el siguiente comando:

```
openssl req -in NombreDelRequest.req -noout -text
```

Presione <Enter> para mostrar los datos del request como se observa en la imagen 10



```
pruebas@BCCR-Ubuntu: ~
-----
pruebas@BCCR-Ubuntu:~$ openssl req -in requestAgente.req -noout -text
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: serialNumber=CPJ-3-101-461460, CN=[3-101-461460] (AGENTE ELECTR
ONICO), OU=CCSS, O=PERSONA JURIDICA, C=CR
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:f4:f9:db:4e:31:e0:95:ea:6f:ff:65:3b:81:04:
      9d:d7:dd:2e:e5:9d:b7:f4:bd:08:ea:00:c8:b8:a9:
      1e:c0:38:12:c1:1e:71:96:06:46:93:e8:83:a0:d8:
      30:88:1e:3c:9b:bd:57:23:fa:a2:23:67:8c:14:b7:
      e8:e1:2a:4c:ab:2a:19:31:f6:3c:47:d0:6c:ed:76:
      75:21:35:97:44:10:a8:c5:93:73:50:0f:44:d1:56:
      c6:60:b6:79:2a:60:35:78:9d:02:6e:d9:ee:59:e4:
      d3:a3:ba:91:d6:4f:8e:cc:d2:5a:26:61:ca:1a:c4:
      08:d0:57:62:37:87:4a:ad:f0:61:75:9e:6e:fe:4a:
      06:39:d3:4c:e6:e5:7e:e9:1f:6f:bf:4e:f7:4f:be:
      ab:20:ec:33:eb:dcc:14:ed:95:1f:b2:b1:a0:e1:8b:
      d3:89:e8:1e:b0:63:09:a2:b6:2f:e8:03:76:58:5b:
      c3:5b:59:0d:a5:f7:b1:a4:5e:19:a0:37:25:9e:92:
      a5:9d:19:15:4b:8e:ca:4d:ab:9a:f5:42:27:27:27:
      3b:4b:87:0d:73:87:65:85:fe:fe:a8:85:20:d0:0c:
      c9:8b:ca:96:0e:1b:17:0a:7d:ed:77:c2:5d:79:6d:
      25:72:26:a3:6d:52:c4:98:d4:28:98:6a:7c:a6:0b:
      35:8b
    Exponent: 65537 (0x10001)
  Attributes:
  Requested Extensions:
    X509v3 Key Usage:
      Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Subject Key Identifier:
      75:0F:D4:F7:4C:BC:E6:49:DF:4C:1F:F0:DA:E3:DC:7B:BE:05:49:76
    X509v3 Subject Alternative Name:
      DNS:www.bccr.fi.cr
  Signature Algorithm: sha1WithRSAEncryption
```

Imagen 10

Parte 5: Anexos

Anexo A. Generar el REQ con una unidad organizacional vinculada a la entidad para sello electrónico

Si usted desea generar un request que posea una unidad organizacional vinculada a la entidad, puede incluir el **atributo opcional "Unidad Organizacional (OU)"**. Si se incluye, **éste debe ser diferente al nombre común de la persona jurídica solicitante (CN) y no debe sobrepasar los 64 caracteres. (esto incluye los 44 caracteres máximos de la razón social y el texto de " (SELLO ELECTRONICO)"**) Por ejemplo, para entidades con personería jurídica instrumental, se debe escribir en la unidad organizacional (**OU**) el **nombre de la unidad organizacional en mayúscula**, y ejecutar el siguiente comando:

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5=CPJ-{#CEDULA JURIDICA#}/CN={#RAZON SOCIAL#} (SELLO ELECTRONICO)/OU={#UNIDAD ORGANIZACIONAL#}/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestSello.req
```

Donde el **id_01** debe reemplazarse por el identificador de la llave privada que se va a utilizar. Por ejemplo:

```
openssl req -new -key llave.key -subj "/2.5.4.5=CPJ-3-101-123456/CN=BANCO BBVA (SELLO ELECTRONICO)/O=PERSONA JURIDICA/C=CR" -out requestSello.req
```

Anexo B. Generar el REQ con una unidad organizacional vinculada a la entidad para agente electrónico

Si usted desea generar un request que posea una unidad organizacional vinculada a la entidad, puede incluir el **atributo opcional "Unidad Organizacional (OU)"**. Si se incluye, **éste debe ser diferente al nombre común de la persona jurídica solicitante (CN) y no debe sobrepasar los 64 caracteres. (esto incluye los 43 caracteres máximos de la razón social y el texto de " (AGENTE ELECTRONICO)"**) Por ejemplo, para entidades con personería jurídica instrumental, se debe escribir en la unidad organizacional (**OU**) el **nombre de la unidad organizacional en mayúscula**, y ejecutar el siguiente comando:

```
openssl req -engine pkcs11 -new -key id_01 -subj "/2.5.4.5=CPJ-{#CEDULA JURIDICA#}/CN={#RAZON SOCIAL#} (AGENTE ELECTRONICO)/OU={#UNIDAD ORGANIZACIONAL#}/O=PERSONA JURIDICA/C=CR" -keyform engine -out requestAgente.req
```