

Instalación de una CA en ubuntu

Lo primero será instalar easy-rsa:

```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Des:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]  
Des:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [163 kB]  
Des:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [235 kB]  
Des:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [899 kB]  
Descargados 63,3 MB en 5s (13,3 MB/s)  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se pueden actualizar 1326 paquetes. Ejecute «apt list --upgradable» para verlos.  
  
(kali㉿kali)-[~]  
$ sudo apt install easy-rsa  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
easy-rsa ya está en su versión más reciente (3.1.0-0.1).  
fijado easy-rsa como instalado manualmente.  
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.  
nvidia-tesla-510-alternative  
Utilice «sudo apt autoremove» para eliminarlo.  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1326 no actualizados.  
  
(kali㉿kali)-[~]  
$
```

Ahora creamos un directorio y creamos un link simbólico al directorio donde se guardará todo. Damos permisos solo al usuario propietario para que nadie mas puede usar nuestra CA para certificar.

```
(kali㉿kali)-[~]  
$ mkdir ~/easy-rsa  
  
(kali㉿kali)-[~]  
$ ln -s /usr/share/easy-rsa/* ~/easy-rsa/  
  
(kali㉿kali)-[~]  
$ chmod 700 /home/kali/easy-rsa
```

Iniciamos el servicio:

```
(kali㉿kali)-[~]  
$ cd ~/easy-rsa  
./easyrsa init-pki  
* Notice:  
  
init-pki complete; you may now create a CA or requests.  
  
Your newly created PKI dir is:  
* /home/kali/easy-rsa/pki  
  
* Notice:  
IMPORTANT: Easy-RSA 'vars' file has now been moved to your PKI above.  
  
(kali㉿kali)-[~/easy-rsa]  
$
```

Creamos el archivo vars dentro de /pki y añadimos la información sobre la CA, es decir, nombre, correo de contacto, país, etc.

```
$ cat pki/vars  
~/easy-rsa/vars  
set_var EASYRSA_REQ_COUNTRY    "ESPAÑITA"  
set_var EASYRSA_REQ_PROVINCE   "MADRIZ"  
set_var EASYRSA_REQ_CITY       "Madrid"  
set_var EASYRSA_REQ_ORG        "Cesar.CA"  
set_var EASYRSA_REQ_EMAIL      "admin@cesar.com"  
set_var EASYRSA_REQ_OU         "Community"  
set_var EASYRSA_ALGO           "ec"  
set_var EASYRSA_DIGEST         "sha512"
```

Creamos una CA, en la cual se nos pedirá una contraseña para cada vez que queramos acceder a ella:

```
(kali@kali)-[~/easy-rsa]
$ ./easyrsa build-ca
* Notice:
Using Easy-RSA configuration from: /home/kali/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Using configuration from /home/kali/easy-rsa/pki/884f44af/temp.d26c5238
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.
_____
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:cesar.ca

* Notice:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/kali/easy-rsa/pki/ca.crt
```

Teóricamente subiríamos la clave publica a internet para que cualquier cliente que quisiera usarla pudiese descargarla. Aquí vamos simplemente a copiarla en otra maquina ubuntu y listo.

```
(kali@kali)-[~/easy-rsa/pki]
$ cat ca.crt
-----BEGIN CERTIFICATE-----
MIIB8zCCAXmgAwIBAgIUMIiU2EzCRZq9M+A3P7z8oBgU4kgwCgYIKoZIzj0EAwQw
EzERMA8GA1UEAwIY2VzYXluY2EwHhcNMjIxMTEzMTE0MDIwWhcNMzIxMTEwMTE0
MDIwWjATMREwDwYDVQQDDAhjZXNhci5jYTB2MBAGByqGSM49AgEGBSuBBAAiA2IA
BFDS5ifWxfi6m6eTaVBekzu+J3YYJNPxxCERJKTJqpLzBoBHPKy2eI2QKxrYBq3V
l+F7LZ80WLNKG9HofofPBP9WgJ9bIc9fVRT6d18qU9gQXAueJbShVBiGNqv3GVSQ
6aOBjTCBijAMBGNVHRMEBTADAQH/MB0GA1UdDgQWB8TMq517yHE8Hb+o343TWUxS
w268MzBOBgNVHSMERzBFgBTMq517yHE8Hb+o343TWUxSw268M6EXpBUwEzERMA8G
A1UEAwIY2VzYXluY2EwGCFDClNhMwkwWavTPgNz+8/KAYFOJIMAsGA1UdDwQEAwIB
BjAKBggqhkhjOPQQDBANoADBIAjB+AOQ/DIwelqOUHGN2hsjjJlZ031LaddVq8tnm
O/bLXXC451rt/fLfuddF20lWqbgCMQDvEmZhpjgfcPuuksEv+fh+NEwE0hWxKWyi
EPxuoRWjFQv9YSp2tLPfkkn/A50s9UE=
-----END CERTIFICATE-----

(kali@kali)-[~/easy-rsa/pki]
$
```

Para ello copiamos el texto y lo pegamos en un nuevo fichero ca.crt.

```
cesar@cesar-virtual-machine: ~  
GNU nano 6.2 /tmp/ca.crt *  
-----BEGIN CERTIFICATE-----  
MIIB8zCCAXmgAwIBAgIUUMiU2EzCRZq9M+A3P7z8oBgU4kgwCgYIKoZIZj0EAwQw  
EzERMA8GA1UEAwYyVzYXlueY2EwHhcNMjIxMTEzMTE0MDIwHcNMzIxMTEwMTE0  
MDIwWjATMREwDwYDVQDDAhjZXNhci5jYTB2MBAGByqGSM49AgEGBSuBBAAiA2IA  
BFDS5ifWxfI6m6eTaVBekzu+J3YYJNPxxCERJKTJqpLzBoBHPKy2eI2QKxrYBq3V  
l+F7LZ80WLNKG9HofPBP9WgJ9bIc9fVRT6d18qU9gQXAueJbShVBiGNqv3GVSQ  
6aOBjTCBijAMBGNVHRMEBTADAQH/MB0GA1UdDgQWBbTMq517yHE8Hb+o343TWUxS  
w268MzB0BgNVHSMERzBFgBTMq517yHE8Hb+o343TWUxSw268M6EXpBUwEzERMA8G  
A1UEAwYyVzYXlueY2GCFDCiLnHmWkVTPgNz+8/KAYFOJIMAsGA1UdDwQEAwIB  
BjAKBggqhkJOPQDBANoADBLAjB+A0Q/DIwelqOUHGN2hsjjJLZ031LaddVq8tnm  
O/bLXXC451rt/fLFuddF20lwqbgCMQDvEmZhpjgfcPuuksEv+fh+NEwE0hwXWyl  
EPxuoRWjFqv9YSp2tLPfkkn/A50s9UE=  
-----END CERTIFICATE-----
```

Ahora añadimos el archivo con la nueva CA a la lista de CAs de la maquina y actualizamos la lista de CAs.

```
cesar@cesar-virtual-machine: ~  
cesar@cesar-virtual-machine:~$ nano /tmp/ca.crt  
cesar@cesar-virtual-machine:~$ sudo cp /tmp/ca.crt /usr/local/share/ca-certific  
ates/  
[sudo] password for cesar:  
cesar@cesar-virtual-machine:~$ sudo update-ca-certificates  
Updating certificates in /etc/ssl/certs...  
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one c  
ertificate or CRL  
1 added, 0 removed; done.  
Running hooks in /etc/ca-certificates/update.d...  
done.  
cesar@cesar-virtual-machine:~$
```

Ahora cada vez que naveguemos por una pagina que este certificada por esta CA el navegador la reconocerá como segura.

Petición de firma de un certificado CSR

Instalamos openssl en el cliente que va a hacer la petición.

```
cesar@cesar-virtual-machine: ~  
Building dependency tree... Done  
Reading state information... Done  
113 packages can be upgraded. Run 'apt list --upgradable' to see them.  
cesar@cesar-virtual-machine:~$ sudo apt install openssl  
E: Invalid operation in  
cesar@cesar-virtual-machine:~$ sudo apt install openssl  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages will be upgraded:  
  openssl  
1 upgraded, 0 newly installed, 0 to remove and 112 not upgraded.  
Need to get 1.183 kB of archives.  
After this operation, 0 B of additional disk space will be used.  
Get:1 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssl amd6  
4 3.0.2-0ubuntu1.7 [1.183 kB]  
Fetched 1.183 kB in 1s (1.525 kB/s)  
(Reading database ... 205820 files and directories currently installed.)  
Preparing to unpack .../openssl_3.0.2-0ubuntu1.7_amd64.deb ...  
Unpacking openssl (3.0.2-0ubuntu1.7) over (3.0.2-0ubuntu1.6) ...  
Setting up openssl (3.0.2-0ubuntu1.7) ...  
Processing triggers for man-db (2.10.2-1) ...
```

Creamos el par de claves para enviar la publica a la CA y que nos firme la petición.

```
cesar@cesar-virtual-machine:~$ cd csr_de_prueba/  
cesar@cesar-virtual-machine:~/csr_de_prueba$ openssl genrsa -out servidor-de-cesar.key  
cesar@cesar-virtual-machine:~/csr_de_prueba$ ls  
servidor-de-cesar.key  
cesar@cesar-virtual-machine:~/csr_de_prueba$ openssl req -new -key servidor-de-cesar.key  
-out servidor-de-cesar.req
```

Ahora creamos la petición CSR con los correspondientes datos para que la CA pueda verificar que somos quienes decimos ser.

```
cesar@cesar-virtual-machine:~/csr_de_prueba$ openssl req -new -key servidor-de-cesar.key  
-out servidor-de-cesar.req  
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) [AU]:ES  
State or Province Name (full name) [Some-State]:mostoles  
Locality Name (eg, city) []:mostoles  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cesario  
Organizational Unit Name (eg, section) []:seccion  
Common Name (e.g. server FQDN or YOUR name) []:servidor-de-cesar  
Email Address []:servidor@cesar.es  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:holaquetal  
An optional company name []:CesarSA  
cesar@cesar-virtual-machine:~/csr_de_prueba$
```

Ahora podríamos mandarles la petición por correo o por cualquier medio que queramos. En este caso lo vamos a hacer mediante ssh, concretamente con scp.

```
cesar@cesar-virtual-machine:~/csr_de_prueba$ scp servidor-de-cesar.req kali@192.168.1.35:/tmp/servidor-de-cesar.req
The authenticity of host '192.168.1.35 (192.168.1.35)' can't be established.
ED25519 key fingerprint is SHA256:DNScALtdQ9N+B+tC8Fx06lx7PVit31s5MrcHrvBNBzM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.35' (ED25519) to the list of known hosts.
kali@192.168.1.35's password:
servidor-de-cesar.req                                100% 1135      1.5MB/s   00:00
cesar@cesar-virtual-machine:~/csr_de_prueba$
```

Ahora desde la CA solo tendríamos que importar la petición a nuestro directorio y firmarla.

```
(kali㉿kali)-[~/easy-rsa]
$ ./easysrsa import-req /tmp/servidor-de-cesar.req servidor-de-cesar
* Notice:
Using Easy-RSA configuration from: /home/kali/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

* Notice:

The request has been successfully imported with a short name of: servidor-de-cesar
You may now use this name to perform signing operations on this request.
```


Captura de firma de solicitud:

```

Archivo Acciones Editar Vista Ayuda

(kali㉿kali)-[~/easy-rsa]
$ ./easyrsa sign-req server servidor-de-cesar
* Notice:
Using Easy-RSA configuration from: /home/kali/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
  countryName           = ES
  stateOrProvinceName   = mostoles
  localityName          = mostoles
  organizationName      = Cesario
  organizationalUnitName = seccion
  commonName            = servidor-de-cesar
  emailAddress          = servidor@cesar.es

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from /home/kali/easy-rsa/pki/4800b2c7/temp.422580f5
Enter pass phrase for /home/kali/easy-rsa/pki/private/ca.key:
403736B0A67F0000:error:0700006C:configuration file routines:NCONF_get_string:no value:../crypto/
conf/conf_lib.c:315:group=<NULL> name=unique_subject
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'ES'
stateOrProvinceName     :ASN.1 12:'mostoles'
localityName            :ASN.1 12:'mostoles'
organizationName        :ASN.1 12:'Cesario'
organizationalUnitName  :ASN.1 12:'seccion'
commonName              :ASN.1 12:'servidor-de-cesar'
emailAddress            :IA5STRING:'servidor@cesar.es'
Certificate is to be certified until Feb 15 12:56:15 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

* Notice:
Certificate created at: /home/kali/easy-rsa/pki/issued/servidor-de-cesar.crt

```

Por ultimo nos faltaría enviar la petición firmada de vuelta al cliente.

[illegible]