Panasonic Electric Works España, S.A.
San Severo, 20, Barajas Park, 28042 Madrid, España
Tel.:+34 902 414 140 • Fax: +34 913 292 976

Número	**ITE0120091**
Título	**FPWEB. OpenVPN. Creación de Certificados**
Versión	**1.0**

0. Sobre Este Documento

Este documento tiene como único objetivo el facilitar la ejecución de las funciones más comunes. En ningún caso, este documento tiene carácter oficial ni se podrá responsabilizar a Panasonic por las erratas o información errónea contenida en el mismo.
Panasonic declina toda responsabilidad por el uso de este documento

1. Descripción

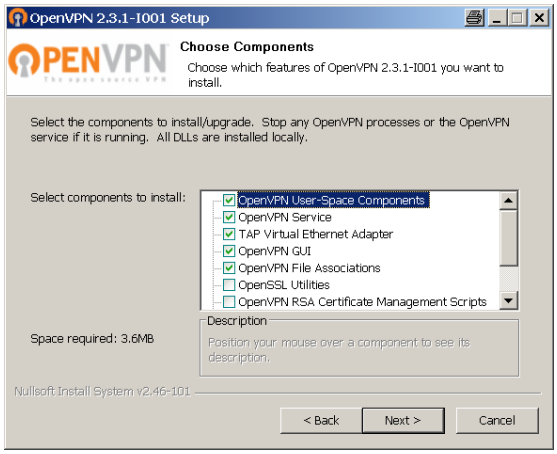
Para realizar una conexión vía OpenVPN se requieren los siguientes certificados y ficheros

Nombre	Necesario para
ca.crt	Certificado común para el servidor y todos los clientes. El nombre es fijo
dh{n}.pem	Fichero con parámetros del servidor. El nombre es fijo
Server.crt	Certificado exclusivo del servidor. El nombre es seleccionable
Server.key	Llave exclusiva del servidor. El nombre es seleccionable
client1.crt	Certificado exclusivo del cliente. Normalmente un certificado distinto por cliente. El nombre es seleccionable
client1.key	Llave exclusiva del cliente. Normalmente una llave distinta por cliente El nombre es seleccionable

Aunque existen muchas formas de crear estos certificados y se pueden encontrar muchos software de creación de certificados, en este informe se detalla cómo crear estos certificados y ficheros de parámetros mediante el software originario de OpenVPN de descarga gratuita desde la página oficial de la comunidad.

www.openvpn.net

Descargue y ejecute el fichero **openvpn-install-2.3.1-I001-i686.exe** para proceder a su instalación. No olvide marcar los elementos OpenSSL Utilities y OpenVPN RSA Certificate Management Scripts que nos permitirán crear los certificados OpenVPN

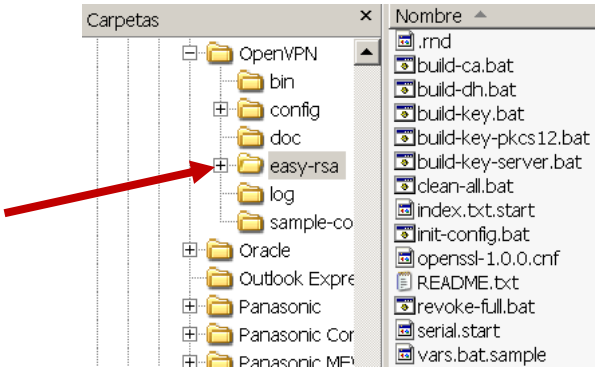


El software se instala por defecto en la ruta:

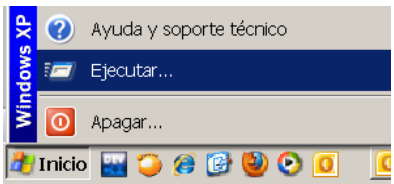
C:\Program Files (o Archivos de Programa)\OpenVPN

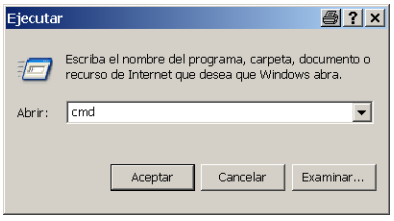
2.- Selección de Claves y Preparativos Previos

En la ruta de acceso donde esté instalado el software OpenVPN existe una carpeta llamada Easy-rsa (normalmente C: \ Archivos de programa \ OpenVPN \ easy-rsa) que contiene varios scripts que al ejecutarlos nos permiten obtener los certificados y claves necesarios (tanto para el servidor como para los clientes) para generar nuestra red OpenVPN.



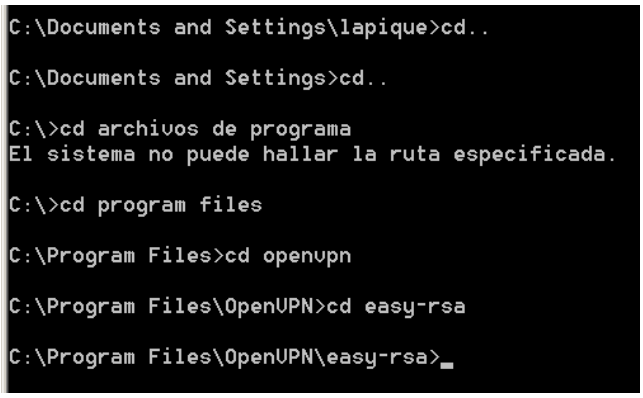
La ejecución de estos scripts se han de realizar necesariamente desde la ventana de comandos de MS-DOS (Inicio-> Ejecutar-> cmd + enter)





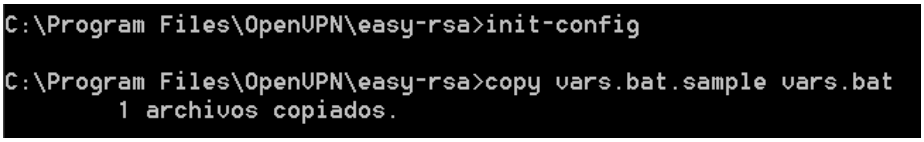
Busque la carpeta Easy-rsa mediante comandos MS-DOS

Nota: Para ir a un nivel inferior en MSDOS (cd..+ enter). Para entrar en una carpeta de ese directorio cd + nombre carpeta (ej. cd Archivos de programa)



En este punto es necesario ejecutar una serie de comandos: El primero de ellos es ***init-config***

Atención, debe estar seguro de que no hay archivos y claves de configuraciones previas existentes, de lo contrario, estos archivos se sobrescribirán inicializándose.



Al ejecutar ***init-config***, se generan dos ficheros ***openssl.cnf*** (en otra ruta) y ***vars.bat*** (en la carpeta Easy-rsa).

Edite el segundo archivo e introduzca algunos parámetros para la creación de las llaves.
Nota: El archivo vars.bat no se edita desde la aplicación de comandos de MS-DOS sino desde un editor de documentos estándar de Windows (Bloc de notas, Wordpad,…).

Las variables que se van a cambiar en la parte final del archivo, personalizándolas apropiadamente con nuestros datos son:

set KEY_COUNTRY=ES
set KEY_PROVINCE=Madrid
set KEY_CITY=Madrid
set KEY_ORG=PanasonicElectricWorks
set KEY_EMAIL=soporte.tecnico@eu.panasonic.com

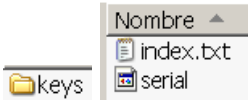
No deje ninguno de estos parámetros en blanco. No deje espacios ni use como separador el carácter “_”
En el caso de KEY_COUNTRY seleccione con 2 letras el país (ES para España)

Inicie de nuevo la aplicación de comando (Inicio-> Ejecutar-> cmd + enter). Generaremos un fichero llamado Index.txt vacío mediante la ejecución (solamente una vez) de los siguientes scripts y en el siguiente orden:

vars
clean-all

```
C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
El sistema no puede hallar el archivo especificado.
        1 archivos copiados.
        1 archivos copiados.
```

Dentro de la carpeta Easy-rsa se generara otra carpeta llamada Keys que contiene dos ficheros recién generados



3.- Obtención del Certificado CA

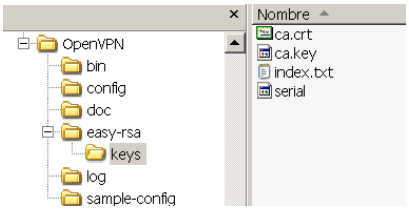
Ahora crearemos el certificado de claves CA (CA: Certification of Authentification), mediante la ejecución (solamente una vez) de:

vars
build-ca

Durante la generación de la clave, se le pedirá una serie de parámetros que se pueden responder confirmando el valor por defecto con la tecla ENTER. Los valores por defecto son los que están definidos en el fichero vars.bat
El único valor que no se debe aceptar por defecto es el de ***Commom Name***. En nuestro caso hemos usado Panasonic pero puede utilizar el nombre que elija.

```
C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.................++++++
writing new private key to 'keys\ca.key'
-----
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) [ES]:
State or Province Name (full name) [Madrid]:
Locality Name (eg, city) [Madrid]:
Organization Name (eg, company) [PanasonicElectricWorks]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]: Panasonic
Email Address [soporte.tecnico@eu.panasonic.com]:

C:\Program Files\OpenVPN\easy-rsa>
```

Al finalizar el proceso, se almacena dentro de la carpeta Keys el certificado CA (***ca.crt***) y la llave del certificado CA (***ca.key***):



El fichero ***ca.crt*** se utilizará tanto en el servidor como en todos los clientes
Importante: El fichero ***ca.key*** se ha de guardar en lugar seguro y no se ha de compartir con nadie. No es necesario en el servidor ni en los clientes.

4.- Obtención del Certificado del Servidor

A continuación procedemos a crear el certificado del servidor ejecutando

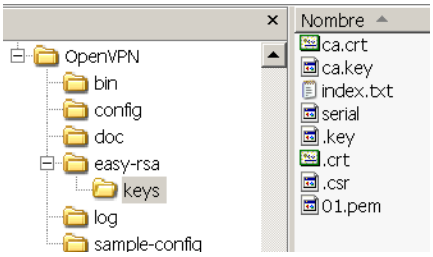
vars
build-key-server

Al igual que antes, se nos pide unos cuantos parámetros que podemos confirmar con Enter. Seleccionamos un nombre para el Commom Name que en este caso será Servidor. Terminamos la ejecución respondiendo YES a la solicitud de firma del certificado y a su guardado.

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'keys\.key'
-----
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) [ES]:
State or Province Name (full name) [Madrid]:
Locality Name (eg, city) [Madrid]:
Organization Name (eg, company) [PanasonicElectricWorks]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:Servidor
Name [changeme]:
Email Address [soporte.tecnico@eu.panasonic.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ES'
stateOrProvinceName   :PRINTABLE:'Madrid'
localityName          :PRINTABLE:'Madrid'
organizationName      :PRINTABLE:'PanasonicElectricWorks'
                      nitName:PRINTABLE
commonName            :PRINTABLE 'Servidor'
                      :PRINTABLE
emailAddress          :IA5STRING:'soporte.tecnico@eu.panasonic.com'
Certificate is to be certified until Jun  1 13:33:23 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

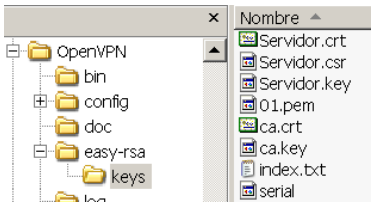
Nota: El Common Name se corresponde con el dominio o nombre DNS del servidor OpenVPN

En la carpeta Keys se me añaden más dicheros teniendo la apariencia:



Normalmente las claves de servidor se generan sin nombre, sólo con una extensión.

Cambiar manualmente el nombre de ellos como ***Servidor.key***, ***Servidor.crt***, ***Servidor.csr***) que es el nombre asignado a la hora de crearlos



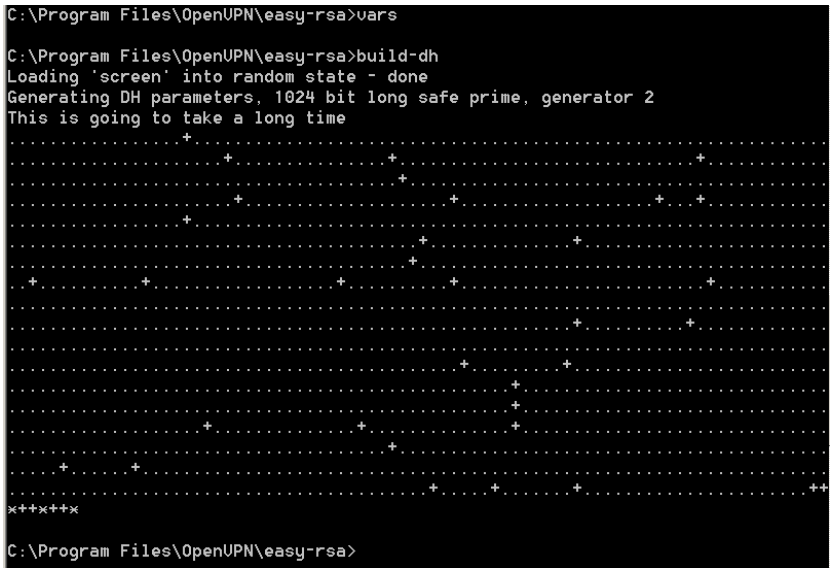
Nota: Se recomienda no dejar espacios ni utilizar el carácter "_" para separar palabras

En el servidor, posteriormente se deberán utilizar los ficheros ***Servidor.key*** y ***Servidor.crt***

5.- Obtención de los Parámetros de Diffie Hellman del Servidor

Los parámetros Diffie Hellman serán utilizados por el servidor OpenVPN. Para generar estos parámetros ejecute los siguientes scripts

vars.bat
build-dh



Este proceso puede tardar algunos minutos. En la carpeta Keys se añade el fichero ***dh1024.pem***.

6.- Obtención de los Certificados de los Clientes

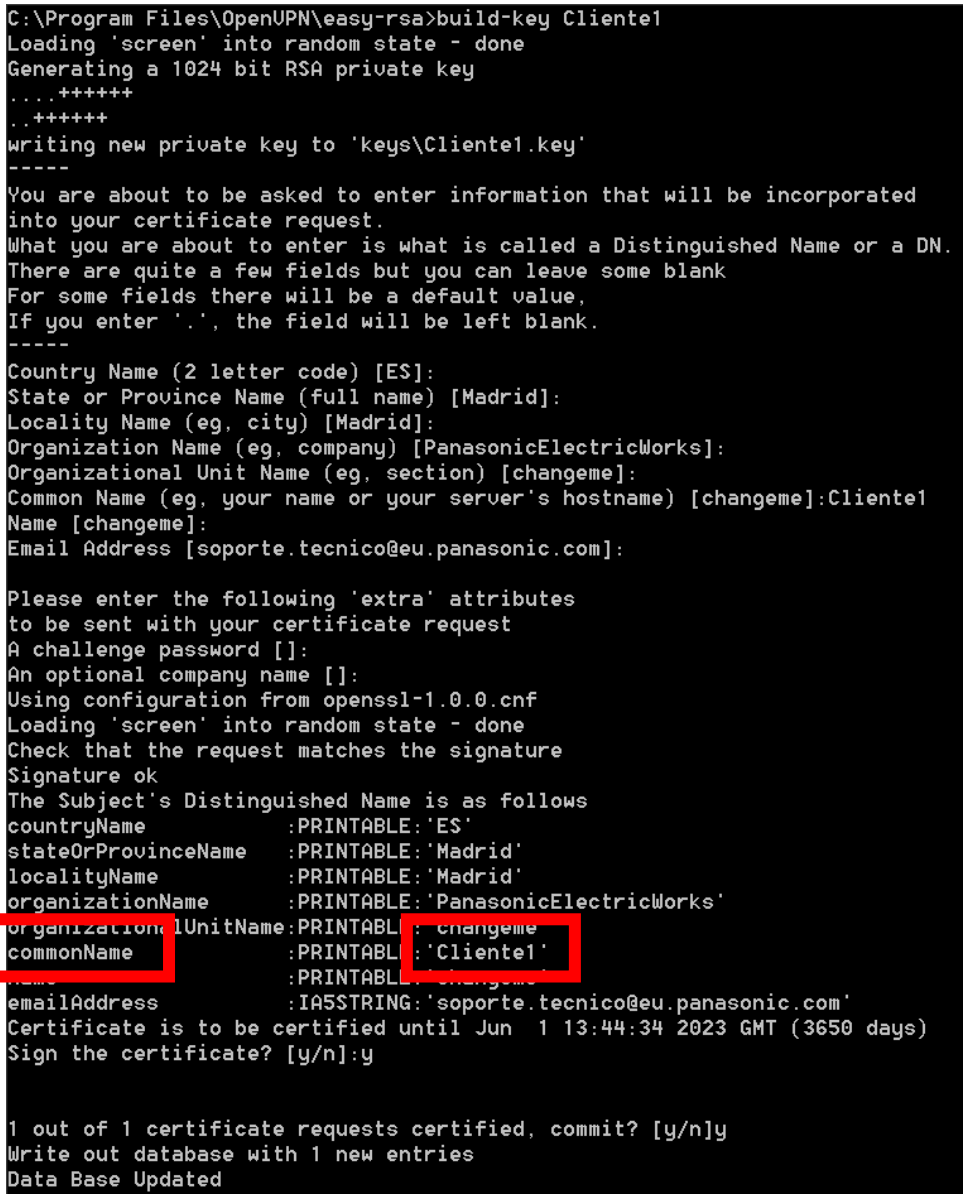
Procedemos a crear el certificado de los clientes ejecutando para cada uno de ellos:

vars

build-key Nombre Cliente

Nota: Se recomienda no dejar espacios ni utilizar el carácter "_" para separar palabras

Seleccionamos un nombre para el **Commom Name** que en este caso será Cliente1. Terminamos la ejecución respondiendo YES a la solicitud de firma del certificado y a su guardado.

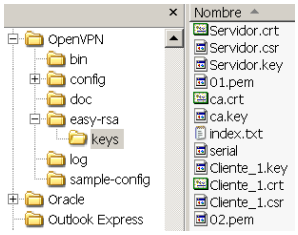


```
C:\Program Files\OpenVPN\easy-rsa>build-key Cliente1
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
....++++++
..++++++
writing new private key to 'keys\Cliente1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate 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) [ES]:
State or Province Name (full name) [Madrid]:
Locality Name (eg, city) [Madrid]:
Organization Name (eg, company) [PanasonicElectricWorks]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:Cliente1
Name [changeme]:
Email Address [soporte.tecnico@eu.panasonic.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ES'
stateOrProvinceName   :PRINTABLE:'Madrid'
localityName          :PRINTABLE:'Madrid'
organizationName      :PRINTABLE:'PanasonicElectricWorks'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'Cliente1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'soporte.tecnico@eu.panasonic.com'
Certificate is to be certified until Jun  1 13:44:34 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Nota: Se recomienda no dejar espacios ni utilizar el carácter "_" para separar palabras

Se harán tantos certificados como clientes se quieran conectar

En la carpeta Keys se me añaden 3 ficheros por cada cliente generado, teniendo la apariencia:



En cada cliente se deberán utilizar los ficheros ***Client_1.key*** y **Cliente_1.crt**

5.- Resumen Creación de Certificados y Claves

Ya hemos generado todas las claves y certificados necesarios para generar la red OpenVPN. De todos los ficheros generados, los necesarios son:

Nombre del fichero	Necesario para	Propósito	Secreto
ca.crt	Servidor + todos los clientes	Certificado de autentificación raíz	NO
ca.key	Sólo para generar más clientes. Guardar en lugar seguro. No entregar ni en el lado del servidor ni en el lado del cliente	Clave de autentificación raíz	SI
dh{n}.pem	Sólo servidor	Parámetros Diffie Hellman	NO
Server.crt	Sólo servidor	Server Certificado	NO
Server.key	Sólo servidor. No compartir con los clientes	Server Key	SI
client1.crt	Sólo cliente	Client1 Certificado	NO
client1.key	Sólo cliente. No compartir con el servidor ni con otros clientes	Client1 Llave	SI

Ayúdenos a Mejorar

Si lo desea puede ponerse en contacto con nosotros en la siguiente dirección de correo:

soporte.tecnico@eu.panasonic.com

Si desea realizar cualquier consulta sobre este informe que no le haya quedado claro, indicar una errata, corregir la información o simplemente evaluar la utilidad de este informe, le rogamos que incluya en el asunto del mail el número del mismo.

Así mismo, estaremos encantados de atender sus solicitudes sobre futuros informes o acciones que considere que Panasonic debería realizar por lo que le ruego utilice este mail como buzón de sugerencias.