


**GENERACIÓN DE  
CLAVES EN  
OPENVPN. GUÍA DE  
CONFIGURACIÓN  
RÁPIDA**

**MANUAL DE USO**

**DAVANTEL**

DESARROLLOS AVANZADOS  
EN TELECOMUNICACIONES, S.L.

Generación de claves en OpenVPN. Guía de Configuración Rápida	
Versión: V1.0spa	
Documento: Generación de claves en OpenVPN. Guía de Configuración Rápida	
Última modificación: 15/12/2010 1:16	
<hr/>	
 <b>DAVANTEL</b> DESARROLLOS AVANZADOS EN TELECOMUNICACIONES, S.L.	C/Pardo 6-8 bajos 08027 Barcelona Tel. +34 933 408 712 Fax. +34 933 401 399 <a href="http://www.davantel.com">http://www.davantel.com</a> <a href="mailto:info@davantel.com">info@davantel.com</a>

# Índice

1. Instalación de OpenVPN.....	4
2. Generación de claves .....	4
2.1. Visión general .....	4
2.2. Generación del certificado master (CA) y su clave .....	4
2.3. Generación del certificado y clave privada para el servidor .....	6
2.4. Generación del certificado y clave privada para los clientes.....	6
2.5. Generación de los parámetros Diffie Hellman.....	7
2.5. Archivos de claves .....	7

## 1. Instalación de OpenVPN

Para generar los certificados y claves tanto para un servidor VPN como para sus clientes es necesario tener instalado el paquete OpenVPN. Este documento describe dicha instalación y posterior uso bajo sistema operativo Windows.

La última versión del paquete OpenVPN puede descargarse del siguiente link

<http://openvpn.net/index.php/open-source/downloads.html>

Se recomienda descargar el instalador de Windows para automatizar dicha instalación sin necesidad de conocimientos específicos del paquete software.

## 2. Generación de claves

### 2.1. Visión general

El primer paso en la construcción de una configuración de claves en OpenVPN 2.0 es establecer una PKI (infraestructura de clave pública). La PKI consta de:

- un certificado independiente (también conocido como una clave pública) y la clave privada para el servidor y cada cliente, y
- un maestro de autoridad de certificación (CA) de certificado y la clave que se utiliza para firmar cada uno de los certificados de servidor y cliente.

OpenVPN admite autenticación bidireccional basada en certificados, lo que significa que el cliente debe autenticar el certificado del servidor y el servidor debe autenticar el certificado de los clientes antes de que se establezca la confianza mutua.

Tanto el servidor como el cliente se autenticarán primeramente verificando que el certificado presentado por el otro fue firmado por la autoridad de certificado patrón (CA). A continuación ambos extremos verificarán la información del encabezado de los certificados verificando el nombre común o el tipo de certificado presentado (cliente o servidor).

Este modelo de seguridad presenta las siguientes ventajas:

- El servidor sólo necesita su propio certificado/clave - no es necesario que conozca los certificados individuales de cada cliente que pueda conectarse
- El servidor sólo aceptará a clientes cuyos certificados fueron firmados con el certificado principal (CA) de la entidad emisora cuya generación veremos más adelante. Y debido a que el servidor puede realizar esta comprobación de la firma sin necesidad de acceso a la clave privada de la entidad emisora de certificados, es posible que la clave de entidad emisora de certificados (la clave más sensible en toda la estructura PKI) que resida una máquina completamente diferente, incluso sin una conexión de red con los elementos de la VPN.
- Si una clave privada está en peligro, puede desactivarse añadiéndose a una CRL (lista de revocación de certificados). La CRL permite rechazar certificados comprometidos de forma individual sin necesidad de tener que regenerar o reconstruir toda la estructura de claves y certificados (PKI).
- El servidor puede gestionar derechos de acceso específicos para diferentes clientes basados en los campos del certificado presentado, tales como el nombre común.

### 2.2. Generación del certificado master (CA) y su clave

En esta sección vamos a generar una certificado/clave de entidad emisora de certificados principal (CA), una clave/certificado de servidor y certificados y claves para 3 clientes diferentes.

Para la administración de PKI, utilizaremos un conjunto de secuencias de comandos con OpenVPN. Para ello, abrir una ventana de símbolo del sistema (Ejecutar cmd) y cambiar al directorio **Archivos de programa\OpenVPN\easy-rsa**. Ejecute el siguiente archivo por lotes para copiar los archivos de configuración en su lugar (este proceso sobrescribirá cualquier archivo **vars.bat** y **openssl.cnf** prexistentes):

### init-config

Ahora, edite el archivo de variables (llamado **vars.bat** en Windows) y configure los parámetros de KEY\_COUNTRY, KEY\_PROVINCE, KEY\_CITY, KEY\_ORG y KEY\_EMAIL. No deje ninguno de estos parámetros en blanco.

A continuación mostramos un ejemplo de archivo **vars.bat**

```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=SP
set KEY_PROVINCE=BCN
set KEY_CITY=Barcelona
set KEY_ORG=DAVANTEL
set KEY_EMAIL=info@davantel.com
```

A continuación inicie la generación de la PKI a través de la secuencia de comandos:

```
vars
clean-all
build-ca
```

El comando final construirá el certificado de la autoridad (CA) de certificación y la clave invocando el comando **openssl**:

```
@echo off
cd %HOME%
rem build a cert authority valid for ten years, starting now
openssl req -days 3650 -nodes -new -x509 -keyout %KEY_DIR%\ca.key -out
%KEY_DIR%\ca.crt -config %KEY_CONFIG%
```

Aparecerá en pantalla los siguientes mensajes mostrando el progreso de la generación del certificado CA y de la clave.

```
ai:easy-rsa # ./build-ca
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '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) [KG]:
State or Province Name (full name) [NA]:
Locality Name (eg, city) [BISHKEK]:
Organization Name (eg, company) [OpenVPN-TEST]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:OpenVPN-CA
Email Address [me@myhost.mydomain]:
```

Si no entramos ningún valor para ningún parámetro, el programa nos tomará los valores definidos en el archivo **vars.bat**. El único parámetro que debe especificarse explícitamente es el **Common Name**. En el ejemplo anterior, utilizamos "OpenVPN-CA".

### 2.3. Generación del certificado y clave privada para el servidor

Para generar el certificado y la clave privada para el servidor entrar el comando

```
build-key-server server
```

Como en el paso anterior, la mayoría de los parámetros pueden tomarse de forma predeterminada a partir del archivo **vars.bat**. Cuando se le pregunte el **Common Name**, escriba "server". Teclee 'y' para responder afirmativamente al resto de preguntas que le haga el proceso de generación.

### 2.4. Generación del certificado y clave privada para los clientes

Para generar los certificados y claves privadas para 3 clientes ejecute los comandos siguientes:

```
build-key client1
build-key client2
build-key client3
```

Para cada cliente, asegúrese de escribir un **Common Name** apropiado cuando se le solicite. Por ejemplo "client1", "client2" y "client3". **Utilice siempre un nombre único para cada cliente.**

## 2.5. Generación de los parámetros Diffie Hellman

Estos parámetros deben generarse únicamente para el servidor. Para hacerlo ejecute el comando:

```
build-dh
```

A continuación aparecerá en pantalla el progreso de la generación tal y como se muestra a continuación:

```
ai:easy-rsa # ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....+.....+.....
.....
```

## 2.5. Archivos de claves

Todos los certificados y claves generados en los pasos anteriores se encontrarán en el subdirectorio **keys**. A continuación los detallamos:

Archivo	Es necesario para...	Significado	Secreto
CA.crt	servidor + todos los clientes	Certificado de entidad emisora de certificados raíz	No
CA.key	sólo equipo firma clave	Clave de entidad emisora de certificados raíz	SÍ
Dh1024.pem	sólo servidor	Parámetros de Diffie Hellman	No
server.crt	sólo servidor	Certificado de servidor	No
server.hey	sólo servidor	Clave de servidor	SÍ
client1.crt	cliente 1 sólo	Certificado de Client1	No
client1.key	cliente 1 sólo	Clave de Client1	SÍ
client2.crt	Cliente 2 sólo	Certificado de Client2	No
client2.key	Cliente 2 sólo	Clave de Client2	SÍ
client3.crt	Cliente 3 sólo	Certificado de client3	No
client3.Key	Cliente 3 sólo	Clave de client3	SÍ

**DAVANTEL**

**DESARROLLOS AVANZADOS  
EN TELECOMUNICACIONES, S.L.**

**BARCELONA**

C./ PARDO 8, BAJOS  
08027 BARCELONA  
TEL.: +34 933 408 712  
FAX: +34 933 401 399

**MADRID**

C./ ARTURO SORIA,320  
28033 MADRID  
TEL.: +34 913 023 758

[www.davantel.com](http://www.davantel.com)

[info@davantel.com](mailto:info@davantel.com)